MASTER'S THESIS

De voorgestelde opsporingsbevoegdheid: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen

Rosema, S.W.

Award date:
2020

Awarding institution:
Department of Criminal Law, International Law and European Law

De voorgestelde opsporingsbevoegdheid: het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen

Naam: S.W. Rosema

Studentnummer: 851524694

Begeleider: mr. M. Visser

Examinator: prof. dr. mr. G.K. Sluiter

Aantal woorden: 13.979

Inleverdatum: 27 oktober 2020

Voorwoord

Voor u ligt mijn scriptie, als afronding van mijn master rechtsgeleerdheid, met als profieldeel strafrecht aan de Open Universiteit. De keuze voor het onderwerp strafrecht in het digitale tijdperk was voor mij een bewuste keuze, omdat strafrecht en ICT mij altijd al fascineerde.

Graag wil ik mijn dank betuigen aan een aantal personen. Allereerst wil ik mijn scriptiebegeleider mr. Mark Visser bedanken voor de plezierige samenwerking en prettige manier van feedback geven. Mijn dank gaat ook uit naar prof. mr. G.K. Sluiter voor het beoordelen van deze scriptie. Daarnaast wil ik mijn gezin, familie, vrienden en collega's hartelijk bedanken voor hun steun.

Sjoerd Willem Rosema

Zwolle, oktober 2020

Inhoud

Lijst van gebruikte afkortingen

aant.	aantekening
A-G	advocaat-generaal
amvb	algemene maatregel van bestuur
art.	artikel
AVG	Algemene verordening gegevensbescherming
Commissie Koops	Commissie modernisering opsporingsonderzoek in het digitale tijdperk
concl.	conclusie
DD	Delikt en Delinkwent
DOI	Digital Object Identifier
e.a.	en anderen
e.v.	en verder
ECLI	European Case Law Identifier
EVRM	Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
EHRM	Europees Hof voor de Rechten van de Mens
HR	Hoge Raad der Nederlanden
JV	Justitiële Verkenningen
m.nt	met noot
MvT	memorie van toelichting
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
OM	openbaar ministerie
OvJ	officier van justitie
p.	pagina
par.	paragraaf
PMSv	Platform Modernisering Stafvordering
Polw	Politiewet 2012
Rb	rechtbank

R-C	rechter-commissaris
r.o.	rechtsoverweging
RMThemis	Rechtsgeleerd Magazijn Themis
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
T&C	Tekst & Commentaar
TvPol	Tijdschrift voor de Politie
TvV	Tijdschrift voor de Veiligheid

Hoofdstuk 1 – Inleiding

§ 1.1 Aanleiding

Op 1 januari 1926 is het huidige Wetboek van Strafvordering tot stand gekomen. Door veranderingen in de samenleving, politiek beleid en technologische ontwikkelingen is dit wetboek sinds die tijd vaak aangepast en bijgewerkt. Tegenwoordig leven we in een wereld waar de digitalisering steeds meer toeneemt, waardoor nieuwe vormen van cybercriminaliteit zijn ontstaan (bijvoorbeeld hacken, identiteitsfraude en phishing).[1] Uit onderzoek is gebleken dat het aantal aangiften van online criminaliteit in 2019 is toegenomen.[2] Zo werd de Universiteit van Maastricht eind december 2019 getroffen door een cyberaanval, waardoor het systeem dagenlang niet goed functioneerde.[3] Onder meer omdat het huidige Wetboek van Strafvordering niet meer optimaal aansluit bij deze vormen van criminaliteit, heeft de regering besloten om het Wetboek van Strafvordering te gaan moderniseren.[4]

Typ op Google je voornaam en achternaam in en binnen enkele seconden verschijnen er allerlei (persoonlijke) gegevens. Gegevens die voor iedereen raadpleegbaar zijn. Opsporingsambtenaren kunnen hier ook handig gebruik van maken. Maar mogen opsporingsambtenaren zomaar allerlei gegevens raadplegen en hier gebruik van maken? Dankzij de social media zijn tegenwoordig veel persoonlijke gegevens online beschikbaar. Als belangrijke oorzaak van deze toename kan het gebruik van smartphones en tablets worden genoemd.[5] Opsporingsambtenaren kunnen bijvoorbeeld via Facebook in de gaten houden op wat voor berichten een persoon heeft gereageerd of welke hij heeft geliket. Aan de hand van deze gegevens kan een sociaal netwerk, zoals een familie- en vriendenkring, van een persoon in kaart worden gebracht. Mensen zijn zich hier vaak niet van bewust en delen allerlei informatie en foto's via het web. Ook zijn er tal van fora en platforms waar mensen onderling informatie en data kunnen uitwisselen.

Mensen delen online bewust of onbewust allerlei informatie. Eenmaal gedeelde informatie blijft vaak circuleren op het internet. Daarbij is het van belang om na te gaan in hoeverre opsporingsambtenaren online informatie mogen overnemen. In toenemende mate wordt in de opsporing gebruik gemaakt van gegevens die afkomstig zijn van het internet. Voor het gebruik hiervan bestaat in het huidige wetboek geen specifieke voorziening. De regering heeft zich dit ook gerealiseerd en om die reden is een nieuw wetsartikel voorgesteld: artikel 2.8.2.4.1. Dit artikel gaat

[1] 'Welke vormen van cybercriminaliteit zijn er?', crisis.nl, 22 september 2020.
[2] Metselaar, 'Aantal geregistreerde misdrijven stijgt, vooral meer online misdaad', *NRC* 15 januari 2020.
[3] Heck, 'Universiteit Maastricht betaalde hackers losgeld' *NRC* 2 januari 2020.
[4] *Kamerstukken II* 2015/16, 29279, nr. 165, p. 1-2; *Kamerstukken II* 2015/16, 29279, nr. 278, p. 1-3.
[5] Van Krieken, *Strafblad*, 2017/14, afl. 4, p. 331.

over het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen.

De opsporingsambtenaar maakt tijdens het onderzoek steeds meer gebruik van informatie die online beschikbaar is. Het overnemen van deze gegevens kan potentiële risico's met zich meebrengen in de sfeer van de privacyschending. Bij de bescherming van de privacy van burgers speelt artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) een centrale rol. Op grond van artikel 94 van de Grondwet wordt een verdrag boven een wet gesteld. Het nationale recht dient in overeenstemming te zijn met, of mag in ieder geval geen schending opleveren van, het Europese recht.[6] Om die reden is het interessant om te bezien of de voorgestelde bepaling in overeenstemming is met het EVRM.

§ 1.2 Hoofdvraag en deelvragen

Naar aanleiding van het voorgestelde wetsartikel wordt in dit onderzoek getracht antwoord te geven op de volgende hoofdvraag: *Is het criterium van stelselmatigheid in het voorgestelde artikel 2.8.2.4.1 uit het Wetboek van Strafvordering voldoende helder en is deze bepaling als geheel in overeenstemming met artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden?*

Om tot een beantwoording van de hoofdvraag te komen wordt deze onderverdeeld in een aantal deelvragen:

- Welke informatie mag de politie op basis van haar algemene taakstelling online vergaren en van welke bijzondere opsporingsbevoegdheden kan daarnaast gebruik worden gemaakt?
- Wat is de achtergrond voor het indienen van het wetsvoorstel?
- Voor welke problematiek beoogt de voorgestelde bepaling een oplossing te creëren?
- Wat is de inhoud en reikwijdte van het begrip stelselmatig?
- Welke eisen worden ex artikel 8 EVRM gesteld aan een gerechtvaardigde inbreuk op de privacy?

§ 1.3 De onderzoeksmethoden

In dit onderzoek wordt gebruik gemaakt van een jurisprudentie- en literatuuronderzoek. Met behulp van een normatief onderzoek wordt in kaart gebracht hoe het recht er uit zou moeten zien. In dit geval wordt onderzocht of het criterium van stelselmatigheid in het voorgestelde artikel 2.8.2.4.1 Wetboek van Strafvordering (hierna: Sv) voldoende helder is en of deze bepaling als geheel in overeenstemming is met artikel 8 EVRM. Het jurisprudentieonderzoek zal zich zowel richten op de

[6] Eijsbouts e.a. 2020, p. 59.

Nederlandse rechtspraak als op de Europese rechtspraak. Eerst wordt aan de hand van de parlementaire geschiedenis, literatuur- en jurisprudentieonderzoek de huidige stand van zaken in Nederland met betrekking tot het overnemen van persoonsgegevens uit publiek toegankelijke bronnen beschreven. Daarna worden het voorgestelde artikel 2.8.2.4.1. Sv en artikel 8 EVRM beschreven en geanalyseerd. Artikel 2.8.2.4.1. Sv zal aan de hand van een literatuuronderzoek worden onderzocht en artikel 8 EVRM zal aan de hand van de parlementaire geschiedenis, literatuur- en jurisprudentieonderzoek van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) worden onderzocht. Tot slot volgt de conclusie met aanbevelingen voor de verdere uitwerking van artikel. 2.8.2.4.1. Sv. Om tot deze aanbevelingen te kunnen komen wordt eerst geanalyseerd of het voorgestelde artikel 2.8.2.4.1. Sv in overeenstemming is met artikel 8 van het EVRM. Onderzocht wordt of door het wetsvoorstel de privacy van burgers kan worden geschonden door onredelijke inmenging in het privéleven door de overheid.

§ 1.4 Opbouw

Om tot een beantwoording van de hoofdvraag te komen wordt deze onderverdeeld in een aantal hoofdstukken. In hoofdstuk 2 wordt de huidige stand van zaken in Nederland met betrekking tot het online vergaren van informatie op internet besproken. Vervolgens wordt in hoofdstuk 3 het voorgestelde artikel 2.8.2.4.1. beschreven en geanalyseerd. Het begrip stelselmatigheid zal uitvoerig aan de orde komen in hoofdstuk 4. In hoofdstuk 5 wordt artikel 8 van het EVRM beschreven en geanalyseerd. Daarnaast wordt aan de hand van het toetsingsschema van het EHRM onderzocht of het wetsvoorstel in overeenstemming is met artikel 8 van het EVRM. Hoofdstuk 6 wordt afgesloten met een conclusie en een aantal aanbevelingen voor de verdere uitwerking van artikel 2.8.2.4.1 Sv.

Hoofdstuk 2 – De huidige rechtspraktijk van informatievergaring via internet

§ 2.1 Inleiding

In dit hoofdstuk wordt de huidige stand van zaken van informatievergaring via internet uiteengezet. Beschreven wordt op basis van welke grondslag op dit moment online informatie mag worden vergaard en welke kritiek daarop valt te leveren. Tot slot wordt in dit hoofdstuk stilgestaan bij de achtergrond voor het indienen van het voorstel voor artikel 2.8.2.4.1 Sv.

§ 2.2 De praktijk

De rechtbank Den Haag heeft op 10 december 2015 een interessante uitspraak gedaan over de huidige stand van zaken met betrekking tot het online overnemen van informatie.[7] Deze rechtszaak staat beter bekend als de Context-zaak. In deze zaak werd onderzoek gedaan naar een organisatie uit Den Haag die zich bezighield met het opruien en ronselen van jongeren die naar Syrië wilden gaan om daar te gaan vechten. De opsporingsambtenaren hielden het Facebook- en Twitteraccount van de organisatie in de gaten om zoveel mogelijk informatie te verzamelen over het netwerk van de verdachten. Tijdens de rechtszaak stelde de advocaat van de verdachten dat de opsporingsambtenaren niet bevoegd waren tot stelselmatige inwinning van informatie. Ex artikel 126j Sv had de officier van justitie (hierna: OvJ) een bevel moeten bevelen.[8] In casu was dat niet gebeurd waardoor in beginsel het recht op privacy uit artikel 8 van het EVRM werd geschonden.[9] Echter oordeelde de rechter dat enige relativering hier noodzakelijk was. De online verzamelde gegevens waren namelijk online voor een ieder toegankelijk waardoor er een minder ernstige situatie ontstond dan wanneer bijvoorbeeld in een afgesloten woning informatie zou worden verzameld.[10] De verdachten wilden juist dat andere mensen hun pagina gingen bezoeken, om zo hun ideologieën kenbaar te maken aan de onlinewereld. Geconcludeerd kan worden dat afhankelijk van de omstandigheden twee grondslagen bestaan voor het inwinnen van online informatie. Dit kan via de algemene taakstelling van de politie of via de bijzondere opsporingsbevoegdheden (specifiek stelselmatige observatie of stelselmatige inwinning van informatie). Niet alleen in deze zaak, maar ook daarbuiten, wordt discussie gevoerd: welke grondslag wanneer gebruiken?[11] In de volgende paragrafen wordt daar nader op ingegaan.

---

[7] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365.
[8] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.27.
[9] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.33.
[10] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.34.
[11] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018; Stol & Strikwerda, *TvV* 2018/17; Veen, *DD* 2019/30.

§ 2.3 De algemene taakstelling van de politie: artikel 3 Polw

Het recht op eerbiediging van het privéleven is gewaarborgd in artikel 8 van het EVRM. In het tweede lid worden een aantal voorwaarden gesteld om hier van af te wijken.[12] Hierbij spelen de proportionaliteit en subsidiariteit een belangrijke rol. Van proportionaliteit is sprake indien een inbreuk op de privacy van een persoon noodzakelijk is en in verband met het algemeen belang van het onderzoek, mag die inbreuk niet groter zijn dan dat de omstandigheden dat rechtvaardigen.[13] Subsidiariteit houdt in dat voor een persoon het minst ingrijpende middel moet worden ingezet om het gewenste doel te kunnen bereiken.[14]

Een belangrijke voorwaarde uit het tweede lid van artikel 8 van het EVRM is dat de inbreuk bij wet is voorzien. In het Nederlandse strafprocesrecht is deze voorwaarde verankerd in het zogeheten legaliteitsbeginsel: "*Strafvordering heeft alleen plaats op de wijze bij de wet voorzien.*"[15] Dit betekent dat een feit pas strafbaar is indien het desbetreffende feit vooraf in een wettelijke bepaling strafbaar is gesteld.[16] Op basis van de artikelen 141 en 142 Sv wordt aan een opsporingsambtenaar die belast is met de opsporing van een strafbaar feit een opsporingsbevoegdheid toegekend. Deze bepalingen komen overeen met de algemene taakstelling van de politie uit artikel 3 van de Politiewet 2012 (hierna: Polw).

In het Zwolsman-arrest[17] geeft de Hoge Raad aan hoe ver de politie mag gaan tot de uitvoering van haar algemene taakstelling. Het moet daarbij gaan om een niet meer dan geringe inbreuk op de persoonlijke levenssfeer van een persoon.[18] Uit de Context-zaak blijkt dat de politie bij het online vergaren van informatie over een persoon gebruik kan maken van de bevoegdheid uit artikel 3 Polw.[19] Belangrijke eis hierbij is dat de online informatievergaring een niet meer dan geringe inbreuk op de privacy van een persoon oplevert. Van geval tot geval wordt dit bezien. Deze werkwijze van de politie wordt zowel in de memorie van toelichting[20] als in de literatuur[21] beschreven. Eveneens wordt dit in de in de rechtspraak bevestigd.[22] Voorwaarde is dat dit niet leidt tot een meer dan geringe inbreuk op iemand zijn privacy en dat de gebruikte opsporingsmethode

[12] Oerlemans, *Investigating Cybercrime* 2017, p. 74-77.
[13] Corstens & Borgers 2018, p. 64.
[14] Corstens & Borgers 2018, p. 64.
[15] Art. 1 Sv.
[16] Keulen & Knigge 2016, p. 23.
[17] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328.
[18] HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, r.o. 6.4.5.
[19] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.18.
[20] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.
[21] Lassche, in: *Digitalisering en de opsporingspraktijk - juridische aspecten*, p. 9 (online, bijgewerkt maart 2019); Stol & Strikwerda, *TvV* 2018/17, p. 10.
[22] HR 13 november 2012, ECLI:NL:HR:2012:BW9338, r.o. 2.6.2.

"*geen bijzondere risico's voor de integriteit en de betrokkenheid van de opsporing in zich heeft.*"[23] Indien sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer dan moet gebruik worden gemaakt van de bijzondere opsporingsbevoegdheden uit het Wetboek van Strafvordering. Specifiek de artikelen 126g (stelselmatige observatie) en 126j (stelselmatige inwinning van informatie) zijn voor het online vergaren van informatie van belang.[24] Deze werkwijze wordt niet expliciet in de wet omschreven, maar wordt wel toegepast in de huidige rechtspraktijk.[25]

Van te voren moeten de OvJ en opsporingsambtenaar bepalen of de algemene taakstelling van de politie of de bijzondere opsporingsbevoegdheid een wettelijke grondslag biedt.[26]

§ 2.4 De artikelen 126g en 126j Sv

Het onderscheid tussen artikel 3 Polw en de artikelen 126g en 126j Sv zit in de vraag of er een meer dan geringe inbreuk op de persoonlijke levenssfeer van een verdachte wordt gemaakt en of die inbreuk al dan niet stelselmatig is. De vraag wanneer er sprake is van een meer dan geringe inbreuk kan aan de hand van een aantal factoren uit de memorie van toelichting en de jurisprudentie worden toegelicht. Per situatie moet beoordeeld worden of er min of meer een volledig beeld over iemand zijn privéleven kan worden verkregen. Factoren die bij stelselmatige observatie een rol spelen zijn: de duur, de plaats, de intensiteit, de frequentie en het eventueel gebruik van een technisch hulpmiddel.[27] Aan de hand van deze factoren wordt per situatie bepaald of er sprake is van stelselmatigheid.[28] Doorslaggevend is of het resultaat van de observatie een min of meer volledig beeld weergeeft over bepaalde aspecten uit iemands privéleven. Hoe langer en vaker de observatie plaatsvindt des te eerder een min of meer een volledig beeld van een persoon wordt verkregen.

Aan de hand van een aantal voorbeelden uit de memorie van toelichting en de jurisprudentie van de Hoge Raad wordt het voorgaande toegelicht. Reden hiervoor is dat de memorie van toelichting naar zijn aard wat algemeen geformuleerd is terwijl de jurisprudentie over concrete casuïstiek gaat. Zo wordt het observeren van een verdachte om zijn (criminele) netwerk in kaart te brengen aangeduid als stelselmatig.[29] In deze situatie kan worden betoogd dat de observatie meerdere malen moet gebeuren teneinde het netwerk in kaart te kunnen brengen.[30] Daarentegen wordt het oppervlakkig in de gaten houden van hangjongeren niet als stelselmatig bestempeld.[31] In

[23] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.15.
[24] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 3.
[25] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 89.
[26] Oerlemans, *Normering van digitale opsporingsmethoden* 2017, p. 32.
[27] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27.
[28] Blom, in: *T&C Sv* 2019, art. 126g Sv, aant. 2 (online, bijgewerkt 1 juli 2019).
[29] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27.
[30] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.18.
[31] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27.

deze situatie kan worden betoogd dat het in de gaten houden elke keer kort was, af en toe plaatsvond en er werd geen technisch hulpmiddel ingezet, zodat het in kaart brengen van het netwerk niet aan de orde was.[32]

In een andere situatie oordeelde de Hoge Raad dat de politie ten behoeve van de algemene taakstelling in de openbare ruimte personen mag observeren, omdat het van korte duur was en de intensiteit laag was.[33] In een zaak over het plaatsen van een peilbaken onder een auto van de verdachte gedurende vijf dagen, oordeelde de Hoge Raad dat er geen sprake was van stelselmatigheid.[34] De auto werd alleen gevolgd als de auto ging rijden en het was slechts van korte duur. Om die reden werd geen min of meer volledig beeld van bepaalde aspecten uit het privéleven van de verdachte verkregen. Afhankelijk van de omstandigheden wordt aan de hand van bovenstaande factoren beoordeeld of er sprake is van stelselmatigheid.

Een ander bijzondere opsporingsbevoegdheid is stelselmatige inwinning van informatie. Hier is bijvoorbeeld sprake van indien een opsporingsambtenaar actief interfereert in het leven van de verdachte.[35] Ook kan informatie worden ingewonnen door middel van bijvoorbeeld cameratoezicht of het plaatsen van een peilbaken onder een auto.[36] Een kenmerkend verschil tussen stelselmatige inwinning van informatie en stelselmatige observatie is dat de opsporingsambtenaar actief infiltreert in de omgeving van de verdachte met als doel zoveel mogelijk informatie te vergaren.[37] Bij observatie is daar in mindere mate sprake van. De wetsgeschiedenis noemt een aantal voorbeelden van stelselmatigheid. Zo kan een opsporingsambtenaar deelnemen aan een sportvereniging of herhaaldelijk naar hetzelfde café gaan, waar een verdachte ook regelmatig naar toe gaat. Daarnaast kan een opsporingsambtenaar deelnemen aan een nieuwsgroep op internet waar een bepaalde persoon aan deelneemt. Een nieuwgroep is een communicatiekanaal op Usenet.[38]

De OvJ en opsporingsambtenaar moeten aan de hand van de factoren uit de memorie van toelichting bepalen of de inbreuk op grond van artikel 3 Polw of de artikelen 126g en 126j Sv kan plaatsvinden. Vanuit de literatuur wordt kritiek geuit op deze werkwijze omdat dit geen rechtlijnig proces is en daardoor beoordelingsruimte ontstaat voor de OvJ en opsporingsambtenaar.[39] Stel er wordt een inschatting gemaakt over de verwachte inbreuk op de privacy van een persoon. Achteraf blijkt deze inschatting onjuist en de inbreuk veel groter te zijn. Ook zijn in de jurisprudentie gevallen

[32] Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.18.
[33] HR 12 mei 2015, ECLI:NL:PHR:2015:1018, r.o. 4.3.
[34] HR 6 november 2018, ECLI:NL:HR:2018:2050, r.o. 2.5.
[35] Blom, in: *T&C Sv* 2019, art. 126j Sv, aant. 1 (online, bijgewerkt 1 juli 2019).
[36] HR 27 november 2012, ECLI:NL:HR:2012:BY0215; HR 6 november 2018, ECLI:NL:HR:2018:2050.
[37] Oerlemans & Koops, *JV* 2012/05, p. 43-44.
[38] Rozendaal & Zuiderveen Borgesius, *Computerrecht* 2017/75, p. 122.
[39] Stol & Strikwerda, *TvV* 2018/17, p. 13-14; Veen, *DD* 2019/30, p. 393.

te vinden waarin de grondslag achteraf niet bleek te kloppen.[40] Indien er sprake is van een niet meer dan geringe inbreuk dan kan artikel 3 Polw als grondslag worden gebruikt. Als er sprake van een meer dan een geringe inbreuk en die inbreuk stelselmatig is, dan kan artikel 126g of artikel 126j Sv als grondslag worden gebruikt. Het verschil in de grondslag is gelegen in het niveau van de rechtsbescherming. Bij een meer dan geringe inbreuk vindt meer bescherming plaats, omdat de OvJ eerst in de vorm van een machtiging toestemming moet verlenen.

§ 2.5 De huidige gang van zaken

Het Openbaar Ministerie (hierna: OM) heeft in samenspraak met de politie een Leidraad Bevoegdheden informatievergaring op internet gepubliceerd. Deze is echter alleen voor opsporingsambtenaren toegankelijk.[41] Stol en Strikwerda hebben een artikel gepubliceerd waarin globaal wordt uitgelegd hoe deze leidraad in de digitale opsporingspraktijk gebruikt kan worden.[42] In de leidraad van het OM staan aanwijzingen wanneer artikel 3 Polw en de artikelen 126g en 126j Sv toegepast kunnen worden bij het online vergaren van informatie door de opsporingsambtenaar. Artikel 3 Polw kan als grondslag worden gebruikt wanneer een opsporingsambtenaar online publiek toegankelijke informatie raadpleegt en er sprake is van een niet meer dan geringe inbreuk op de privacy van een persoon. Gaat de opsporingsambtenaar actief op zoek naar online publiek toegankelijke informatie en levert die inbreuk een min of meer volledig beeld van een persoon op dan kunnen de artikelen 126g of 126j Sv als grondslag worden gebruikt.

Het vaststellen van een grondslag op basis van artikel 3 Polw en de artikelen 126g of 126j Sv blijft in zijn algemeenheid een lastige kwestie. Het begrip stelselmatigheid wordt als kantelpunt gebruikt om te bepalen of er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer van een persoon. Hieruit blijkt dat niet altijd duidelijk is welke opsporingshandelingen tot welke gevolgen leiden en bijgevolg wanneer welke grondslag gekozen moet worden.[43] Aan de hand van de factoren duur, intensiteit, frequentie en het eventueel gebruik van een technisch hulpmiddel kan dit worden bepaald. Op basis van de jurisprudentie[44] en literatuur[45] kan geconcludeerd worden dat de huidige regelgeving met betrekking tot stelselmatige inwinning van informatie het beste aansluit bij het online vergaren van informatie in de hedendaagse opsporingspraktijk. Reden hiervoor is: ”*dat bij het verzamelen van informatie over een persoon op internet niet zozeer sprake is van het*

[40] HR 6 november 2018, ECLI:NL:HR:2018:2050; HR 9 september 2014, ECLI:NL:HR:2014:2650.
[41] Stol, *TvPol.* 2018/80, p. 24.
[42] Stol & Strikwerda, *TvV* 2018/17, p. 11.
[43] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 46.
[44] HR 18 juni 2019, ECLI:NL:PHR:2019:648, r.o. 74; Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248.
[45] Lassche, in: *Digitalisering en de opsporingspraktijk - juridische aspecten*, p. 11 (online, bijgewerkt maart 2019); Stol & Strikwerda, *TvV* 2018/17, p. 13-14.

volgen van een persoon of van het waarnemen van diens aanwezigheid of gedrag als bedoeld in 126g Sv omdat deze persoon niet feitelijk wordt waargenomen."[46] Hieruit volgt dat stelselmatig observeren niet goed tot zijn recht komt. Bij het online vergaren van informatie wordt namelijk geen persoon of gedrag waargenomen maar worden online gegevens geraadpleegd. Bij stelselmatige inwinning van informatie is daar in zekere zin minder sprake van.[47]

Indien een onderzoek gaat plaatsvinden naar online publiek toegankelijke informatie dan kan de OvJ in de huidige opsporingspraktijk een bevel tot stelselmatige inwinning van informatie of een bevel tot stelselmatige observatie geven.[48] Dit wordt bevestigd in de memorie van toelichting.[49] Bij deze werkwijze kunnen vraagtekens worden gezet. Een bijkomend probleem is dat blijkens de wetgeschiedenis sprake moet zijn van misleiding. Echter hoeft hier niet altijd sprake van te zijn. Een opsporingsambtenaar hoeft bijvoorbeeld bij het raadplegen van online publiek toegankelijke informatie niet undercover te gaan, omdat hij geen persoonlijk contact hoeft te maken met de verdachte. In de regel is hier geen sprake van 'misleiding', terwijl dit wel als eis wordt gesteld in de wetsgeschiedenis. Een ander bijkomend probleem is dat bij stelselmatige observatie sprake moet zijn van een 'realtime element'.[50] Dit betekent dat een verdachte onmiddellijk geobserveerd kan worden in zijn doen en laten. Het gaat dan met name om het feit wat op dat moment wordt waargenomen en wordt vastgelegd. Bij het onderzoek naar persoonsgegeven op internet gaat het vooral om historische gegevens die worden vastgelegd en die voor iedereen toegankelijk zijn. Hierdoor is er geen sprake van een 'realtime element'. Op basis van bovenstaande bevindingen acht de regering dat het noodzakelijk is dat een expliciete wettelijke grondslag komt voor opsporingsambtenaren die stelselmatig onderzoek doen naar persoonlijke gegevens op internet. Als belangrijke oorzaak kan de behoefte uit het werkveld worden genoemd. Door veranderingen in de samenleving en met name door technologische ontwikkelingen sluiten de huidige wetsbepalingen niet goed aan bij het huidige digitale tijdperk.[51] Op basis van deze ontwikkelingen heeft de regering een voorstel ingediend: artikel 2.8.2.4.1 Sv.

---

[46] Lassche, in: *Digitalisering en de opsporingspraktijk - juridische aspecten*, p. 11 (online, bijgewerkt maart 2019).
[47] Stol & Strikwerda, *TvV* 2018/17, p. 14.
[48] Lassche, in: *Digitalisering en de opsporingspraktijk - juridische aspecten*, p. 11 (online, bijgewerkt maart 2019).
[49] *Kamerstukken II* 2016/17, 34720, nr. 3, p. 5; *Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering (Het opsporingsonderzoek)* 2017, p. 89.
[50] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 60.
[51] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.

§ 2.6 Samenvatting

Indien online informatie vergaring leidt tot een niet meer dan geringe inbreuk op de privacy van een persoon dan kan artikel 3 Polw als grondslag worden gebruikt. Is er sprake van een meer dan geringe inbreuk op de privacy van een persoon dan kunnen de artikelen 126g Sv (stelselmatige observatie) of 126j Sv (stelselmatige inwinning van informatie) als grondslag worden gebruikt. Stelselmatigheid speelt een belangrijke rol bij de beoordeling of er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer van een persoon. Echter bij de toepassing van de factoren uit de memorie van toelichting kunnen problemen ontstaan. Dit komt omdat er geen rechtlijnig proces is waardoor er voor de OvJ en opsporingsambtenaar een beoordelingsruimte ontstaat. Het kan voorkomen dat achteraf blijkt dat een verkeerde inschatting is gemaakt over de verwachte inbreuk. De factoren duur, intensiteit, frequentie en het eventueel gebruik van een technisch hulpmiddel sluiten dan ook niet goed aan bij de huidige werkwijze om de stelselmatigheid vast te stellen. Er zullen nieuwe factoren ontwikkeld moeten worden om de stelselmatigheid adequaat te kunnen vaststellen. Tot slot verdient op grond van de jurisprudentie en literatuur een bevel tot stelselmatige inwinning de voorkeur bij het online vergaren van informatie. Reden hiervoor is dat bij stelselmatige observatie sprake moet zijn van een ‘realtime element’, terwijl gegevens op internet vooral van historische aard zijn.

Op dit moment bevat het huidige Wetboek van Strafvordering nog geen expliciete grondslag voor de opsporingsambtenaar voor het online verzamelen van persoonsgegevens via internet. Om aansluiting te kunnen behouden met deze maatschappelijke en technologische ontwikkelingen van de 21ste eeuw heeft de regering een wetsvoorstel ingediend: artikel 2.8.2.4.1 Sv.

Hoofdstuk 3 – De inhoud en reikwijdte van het wetsvoorstel

§ 3.1 Inleiding

De regering heeft een wetsvoorstel ingediend: artikel 2.8.2.4.1 Sv. In dit hoofdstuk wordt de inhoud en reikwijdte van het wetsvoorstel geanalyseerd en beschreven. Daarnaast wordt stilgestaan bij het verdenkingscriteria en het voorlopige hechteniscriterium.

§ 3.2 De inhoud en reikwijdte

De regering heeft het voorgestelde artikel 2.8.2.4.1 Sv als volgt omschreven:
"1. In geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld, kan de officier van justitie bevelen dat een opsporingsambtenaar stelselmatig, al dan niet op geautomatiseerde wijze persoonsgegevens uit publiek toegankelijke bronnen overneemt.
2. Het bevel wordt gegeven voor een periode van ten hoogste drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd.
3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de geautomatiseerde wijze van overnemen van gegevens."[52]

Het wetsvoorstel omvat een aantal verschillende onderwerpen. Allereerst wordt ingegaan op de voorwaarden waaronder gebruik kan worden gemaakt van de nieuwe opsporingsbevoegdheid. Vervolgens wordt ingegaan op een aantal bestanddelen uit het wetsvoorstel.

Bij verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van een jaar of meer is gesteld kan de OvJ bevelen dat een opsporingsambtenaar stelselmatig, al dan niet op geautomatiseerde wijze, persoonsgegevens uit publiek toegankelijke bronnen kan overnemen. In zijn onderzoek naar digitale opsporing merkt Veen daarbij op dat bij toepassing van dit bevel niet aan het 'verdachtebegrip' hoeft te worden voldaan.[53] Dit impliceert dat bij een onderzoek niet alleen gegevens van verdachten kunnen worden onderzocht, maar ook van personen die niet verdacht zijn. In de opsporingspraktijk zou dit kunnen betekenen dat de persoonsgegevens van een grote groep mensen kan worden geraadpleegd. Het is maar de vraag of dit overeenkomst met het recht op privacy uit artikel 8 van het EVRM. Dit aspect zal nader worden beschouwd in hoofdstuk 5.

[52] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 7-8; *Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 60.
[53] Veen, *DD* 2019/30, p. 401.

In de huidige rechtspraktijk wordt bij een groot aantal opsporingsbevoegdheden gebruik gemaakt van het voorlopige hechteniscriterium.[54] Van deze bevoegdheid kan alleen worden gebruik gemaakt indien is voldaan aan het criterium uit artikel 67 Sv. Dit houdt in dat alleen van een opsporingsbevoegdheid gebruik kan worden gemaakt indien er sprake is van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld.[55] Daarnaast is een bevel tot voorlopige hechtenis op een aantal specifieke strafbare feiten toegestaan.[56] De regering erkent dat het criterium een aantal nadelen heeft.[57] Vanuit dat oogpunt worden in het nieuwe Wetboek van Strafvordering verdenkingscriteria geïntroduceerd. Deze criteria zullen in beginsel bestaan uit een eenjaarscriterium en wanneer de bevoegdheid ingrijpender is uit een vierjaarscriterium.[58] In het kader van de overzichtelijkheid van de verdenkingscriteria is de voorgestelde criteria eenvoudiger en duidelijker geworden. Het voorlopige hechteniscriterium is namelijk te ver doorgeschoten waardoor er te veel differentiatie is ontstaan.[59]

Uit de memorie van toelichting volgt dat de bevoegdheid van artikel 2.8.2.4.1 Sv alleen kan worden gebruikt als is voldaan aan de eisen van proportionaliteit en subsidiariteit.[60] De regering heeft deze beginselen nu verankerd in artikel 2.1.2.2 Sv.[61] Eerst moet aan de hand van het proportionaliteitsbeginsel worden beoordeeld of de uitoefening van de bevoegdheid in redelijke verhouding staat tot het beoogde doel.[62] Aan de hand van het subsidiariteitsbeginsel wordt beoordeeld of het minst ingrijpende middel kan worden ingezet om een bepaald doel te kunnen bereiken.[63]

Stelselmatigheid

Artikel 2.8.2.4.1 Sv geeft de bevoegdheid om stelselmatig gegevens over te nemen via publiek toegankelijke bronnen. Hiervan is sprake als "*daarbij op voorhand redelijkerwijs voorzienbaar een*

[54] Keulen & Knigge 2016, p. 356-357.
[55] Art. 67 lid 1 sub a Sv.
[56] Art. 67 lid 1 sub b Sv; art. 67 lid 1 sub c Sv.
[57] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 12.
[58] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 13.
[59] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 12.
[60] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 18.
[61] *Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 5.
[62] Corstens & Borgers 2018, p. 438.
[63] Corstens & Borgers 2018, p. 438.

min of meer volledig beeld kan worden verkregen van bepaalde aspecten van iemands privéleven."[64] Het begrip stelselmatigheid blijft ten aanzien van de huidige rechtssituatie vrijwel ongewijzigd. Zo zal bij het raadplegen van het sociale netwerk van een persoon op Facebook een min of meer volledig beeld worden verkregen van bepaalde aspecten uit zijn persoonlijke leven. De Commissie modernisering opsporingsonderzoek in het digitale tijdperk (hierna: Commissie Koops) heeft onderzoek gedaan naar de digitale ontwikkelingen die spelen in opsporingsonderzoeken. De Commissie Koops heeft een algemeen normeringscriterium opgesteld voor het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen:
"1. niet-stelselmatige uitoefening van een bevoegdheid is mogelijk door een opsporingsambtenaar
2. voor stelselmatige uitoefening van een bevoegdheid is in de regel een bevel van de officier van justitie nodig; stelselmatig betekent dat bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan;
3. voor ingrijpend stelselmatige uitoefening van een bevoegdheid is een machtiging van de rechter-commissaris nodig; ingrijpend stelselmatig betekent dat bij de uitoefening van een bevoegdheid op voorhand redelijkerwijs voorzienbaar een ingrijpend beeld van iemands privéleven kan ontstaan."[65]

Aan de hand van bovenstaande criteria moet per situatie beoordeeld worden of er sprake is van stelselmatigheid. Deze criteria zijn door de wetgever overgenomen.[66] Daarnaast kan in tegenstelling tot stelselmatige observatie en stelselmatige inwinning van informatie bij de uitvoering van de bevoegdheid uit artikel 2.8.2.4.1 Sv gebruik worden gemaakt van historische gegevens op een bepaalde website.[67] Het begrip stelselmatigheid uit de artikelen 126g en 126j Sv speelt een belangrijke rol bij de beoordeling of er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer. Op basis van het smartphone-arrest[68] kan het begrip stelselmatigheid ook worden toegepast bij digitale doorzoekings- en beslagbevoegdheden. Zo oordeelde de Hoge Raad dat het in beslag nemen van een smartphone een geringe inbreuk op de privacy van een persoon opleverde en dat een opsporingsambtenaar op grond van de artikelen 94, 95 en 96 Sv hiertoe zelfstandig bevoegd was.[69] Bij het onderzoek naar persoonlijke gegevens in een digitale omgeving kan op advies van de

[64] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 22; Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.
[65] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 41.
[66] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 3.
[67] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[68] HR 4 april 2017, ECLI:NL:HR:2017:584.
[69] HR 4 april 2017, ECLI:NL:HR:2017:584, r.o. 2.6-2.8.

Commissie Koops onderscheid worden gemaakt tussen geringe, meer dan geringe en zeer ingrijpende inbreuken op het recht op privacy.[70] Als er sprake is van een geringe inbreuk dan hoeft een opsporingsambtenaar geen bevel aan te vragen bij de OvJ. Bij een meer dan geringe inbreuk dient de OvJ een bevel af te geven en bij een zeer ingrijpende inbreuk dient een R-C een bevel af te geven. In hoofdstuk 4 zal het begrip stelselmatigheid nader worden geanalyseerd en beschreven.

Al dan niet op geautomatiseerde wijze

Het derde lid van artikel 2.8.2.4.1 Sv schrijft voor dat bij algemene maatregel van bestuur nadere regels worden gesteld over de geautomatiseerde wijze van overnemen van gegevens.[71] Vooral: "*met het oog op de integriteit en authenticiteit van de overgenomen resultaten*"[72] is dit van belang. De opsporingsambtenaar kan bijvoorbeeld in zijn zoektocht naar persoonlijke gegevens van een willekeurig persoon op internet gebruik maken van een webcrawler.[73] Dankzij deze geautomatiseerde wijze van zoeken is het mogelijk dat eerder dan voorheen een inbreuk wordt gemaakt op de privacy van een persoon. Binnen een korte tijd kan namelijk een grote hoeveelheid persoonsgegevens van een persoon worden geraadpleegd. Op dit moment is de regering bezig met de voorbereiding van de voorschriften van de algemene maatregel van bestuur.[74]

Publiek toegankelijke bronnen

Het is van belang om na te gaan wanneer er sprake is van een publiek toegankelijke bron. In de memorie van toelichting wordt een aantal kenmerken van publiek toegankelijke bronnen genoemd. Zo moet een onbeperkt aantal mensen toegang kunnen krijgen tot de bron zonder dat er een registratie en goedkeuring van een derde hoeft plaats te vinden. Als een registratie geautomatiseerd kan plaatsvinden is er ook sprake van publiek toegankelijke bron. Indien een uitnodiging of goedkeuring is vereist om toegang te verkrijgen tot een bepaalde bron is er geen sprake van een publiek toegankelijke bron.[75] Een voorbeeld hiervan is het versturen van een vriendschapsverzoek via Facebook of toegang aanvragen van een afgeschermd forum of nieuwsgroep. Beslissend is of de gegevens voor een ieder toegankelijk zijn en er geen toestemming van een derde nodig is. De memorie van toelichting geeft een voorbeeld van een internetgebruiker die doelbewust foto's en

[70] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 36.
[71] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 8.
[72] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 46.
[73] Stol & Strikwerda 2017, p. 295.
[74] Brief van de Minister van Justitie en Veiligheid van 9 april 2019 (*Kamerstukken II* 2018/19, 29279, nr. 501, p. 2).
[75] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 245.

filmpjes op een openbare website plaatst.[76] Het is evident dat hier sprake is van een publiek toegankelijke bron, omdat in dit geval de foto's en filmpjes voor een ieder toegankelijk zijn.

De termijn

In het tweede lid van artikel 2.8.2.4.1 Sv wordt een bevel gegeven voor een periode van ten hoogste drie maanden. Daarnaast kan de termijn telkens met een periode van drie maanden worden verlengd.[77] Noch in de memorie van toelichting[78] noch in de consultatieversie van het conceptwetsvoorstel[79] wordt vermeld hoe vaak die termijn kan worden verlengd. In theorie zou de verlenging eindeloos kunnen plaatsvinden.[80] Echter is het wel zo dat de OvJ een toelichting moet geven op zijn genomen besluit.

§ 3.3 Samenvatting

In dit hoofdstuk zijn de hoofdlijnen van artikel 2.8.2.4.1 Sv weergegeven. De regering hanteert in het wetsvoorstel niet meer het voorlopige hechteniscriterium. Nu wordt een grens gelegd bij strafbare feiten waarop een gevangenisstraf van een jaar of meer is gesteld. Het gevolg is nu dat de opsporingsbevoegdheid uit artikel 2.8.2.4.1 Sv vaker bij strafbare feiten kan worden toegepast.

[76] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 245.
[77] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 60.
[78] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[79] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 46.
[80] Veen, *DD* 2019/30, p. 403-404.

Hoofdstuk 4 – Analyse van het wetsvoorstel

§ 4.1 Inleiding

Zowel in de huidige als in de voorgestelde situatie heeft het begrip stelselmatigheid een belangrijke rol bij het overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Derhalve vindt in dit hoofdstuk een uitvoerige analyse van dit begrip plaats.

§ 4.2 De opsporingsbevoegdheid uit artikel 2.8.2.4.1 Sv

De OvJ is belast met de opsporing en vervolging van strafbare feiten.[81] Hij moet zorgen voor een zorgvuldige afhandeling en de opsporingsprocedure moet conform de wet verlopen. De OvJ kan ex artikel 2.8.2.4.1 Sv bevelen dat een opsporingsambtenaar stelselmatig persoonsgegevens uit publiek toegankelijke bronnen kan overnemen. De reikwijdte van deze opsporingsbevoegdheid wordt beperkt door het eenjaarscriterium.[82] Dit betekent dat de OvJ in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld een opsporingsbevoegdheid kan bevelen.

Doordat de regering in het wetsvoorstel het eenjaarscriterium hanteert, kan de opsporingsbevoegdheid voor een enorm aantal strafbare feiten worden gebruikt. In de huidige situatie wordt bij de bijzondere opsporingsbevoegdheden het voorlopige hechteniscriterium gehanteerd die uit vier jaar bestaat.[83] Dit houdt in dat de reikwijdte van artikel 2.8.2.4.1 Sv groter is dan artikel 126 e.v. Sv. Een voorbeeld. Stel iemand dient een valse aangifte van een strafbaar feit in.[84] Op basis van dit strafbare feit kan de OvJ ex artikel 2.8.2.4.1 Sv een opsporingsbevoegdheid bevelen, terwijl dit op grond van artikel 126 e.v. Sv niet kan, omdat daar als voorwaarde het voorlopige hechteniscriterium wordt gehanteerd. Ondanks dat de reikwijdte van artikel 2.8.2.4.1 Sv nu groter is geworden, is het de OvJ die de opsporingsbevoegdheid kan bevelen.[85] Ligthart merkt op dat de regering lijkt aan te geven dat bij het overnemen van persoonsgegevens via publiek toegankelijke bronnen geen sprake kan zijn van ingrijpende stelselmatigheid.[86] Derhalve is de OvJ bevoegd om een opsporingsbevoegdheid te bevelen. Veen is van mening dat het de voorkeur geniet dat de R-C een machtiging moet verlenen om zo het eenjaarscriterium te compenseren.[87] Ik ben van

[81] Keulen & Knigge 2016, p. 158.
[82] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 13.
[83] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 12.
[84] Art. 188 Sr.
[85] Simmelink, *RMThemis* 2017, p. 325.
[86] Ligthart, *RMThemis* 2019, p. 196-197.
[87] Veen, *DD* 2019/30, p. 402.

mening dat de genoemde auteurs het deels bij het juiste eind hebben. Doordat het gebruik van internet de laatste jaren flink is toegenomen en daardoor een grote hoeveelheid persoonlijke informatie via publiek toegankelijke bronnen beschikbaar is, kan er namelijk al vrij snel sprake zijn van een (ingrijpende) stelselmatigheid. De R-C kan dan uiteindelijk beoordelen of een machtiging moet worden verleend.

§ 4.3 Het begrip stelselmatigheid in relatie tot artikel 2.8.2.4.1 Sv

In hoofdstuk 2 paragraaf 4 heb ik de factoren genoemd die gebruikt worden bij de beoordeling om de stelselmatigheid vast te stellen. Oerlemans is van mening dat deze factoren niet goed aansluiten bij het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen.[88] Deze constatering is terecht, want factoren als duur, plaats en frequentie zijn niet langer relevant.[89] Zo heeft de plaats weinig relevantie voor het onderzoek naar publiek toegankelijke bronnen en kan tegenwoordig binnen enkele seconden ontzettend veel persoonlijke gegevens worden geraadpleegd, waardoor de duur niet meer relevant is.[90] Om deze redenen worden in de memorie van toelichting en in het onderzoeksrapport van de Commissie Koops een aantal nieuwe factoren voorgesteld.

Bij het vaststellen van de stelselmatigheid komt de Commissie Koops met maar liefst zeventien factoren die worden geclusterd in de volgende categorieën: (1) omvang en type van de (over te nemen) gegevens, (2) aard van de bron, (3) wijze van zoeken en (4) het gebruik van gegevens en de mogelijke impact op de persoon.[91] De Commissie Koops had een kortere lijst van factoren overwogen, maar heeft daar van afgezien: *"omdat dit een te grofmazig afwegingskader zou opleveren, dat in voorkomende gevallen teveel ten koste van de rechtsbescherming zou kunnen gaan."*[92] Duidelijk is dat per situatie een goede afweging gemaakt moet worden.

De factoren van de Commissie Koops zijn ten aanzien van de factoren uit de memorie van toelichting nader uitgesplitst maar komen in grote lijnen overeen. Zo wordt nu meer nadruk gelegd op de wijze van zoeken, de hoeveelheid gegevens die beschikbaar zijn, de geavanceerde manier waarop resultaten door een technisch hulpmiddel vastgelegd worden en de diversiteit van gegevens.[93] Daarnaast noemt de memorie van toelichting nog twee andere factoren: het doel van de

---

[88] Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *PMSv,* 2018/02, DOI: 10.5553/PMSV/258950952018001018001.
[89] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 162.
[90] Ligthart, *RMThemis* 2019, p. 197.
[91] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 163-164.
[92] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 164.
[93] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.

zoekactie en de aard van de persoonsgegevens.[94] Bovenstaande factoren verdienen een nadere toelichting.

Wijze van zoeken

Bij de factor de wijze van zoeken gaat het om de manier van zoeken. Zo kan een opsporingsambtenaar persoonsgericht en beperkt zoeken tegenover persoonsgericht en diep zoeken. Daarbij is vooral de specificiteit van de zoekvraag van belang.[95] Gaat het bijvoorbeeld om een algemene of een specifieke vraag? Bij de wijze van zoeken kan het vaststellen van stelselmatigheid lastig zijn. Stol en Strikwerda wijzen erop dat een eenmalige zoekvraag stelselmatigheid kan opleveren en kan het raadplegen van een grote hoeveelheid informatie geen stelselmatigheid op leveren.[96] De beoordeling van de wijze van zoeken levert op grond van het voorgaande geen doorslaggevende aanwijzing op voor het vaststellen van de stelselmatigheid.

Hoeveelheid informatie

De potentiële hoeveelheid informatie die tegenwoordig via internet kan worden gevonden is enorm. Zo kunnen alle persoonlijke gegevens worden geraadpleegd die door mensen online zijn gezet. Soms worden gegevens op een publiek toegankelijke bron gepubliceerd, zonder dat het de bedoeling was dat de gegevens in brede kring zouden worden geraadpleegd.[97] Met een paar muisklikken kan in een mum van tijd een grote hoeveelheid informatie online worden geraadpleegd.[98] Daarnaast is het op voorhand vrijwel onbekend wat over een persoon kan worden gevonden. Sommige mensen delen online heel veel informatie en anderen vrijwel niets. Op voorhand valt dit nauwelijks te controleren.

Geavanceerd

Met behulp van een technisch hulpmiddel kunnen op geavanceerde wijze resultaten worden vastgelegd. Dit kan zowel handmatig als geautomatiseerd plaatsvinden. Handmatig zoeken kan bijvoorbeeld via een standaard zoekmachine en geautomatiseerd zoeken kan via een webcrawler.[99] Een webcrawler is een programma dat geautomatiseerd alle beschikbare informatie over een persoon van het internet als het ware afschraapt. Doordat dit geautomatiseerd plaatsvindt en dus

---

[94] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[95] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 164.
[96] Stol & Strikwerda, *TvV* 2018/17, p. 11.
[97] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 203.
[98] Moerman, *NJB* 2019/94, p. 113-114.
[99] Stol & Strikwerda, *TvV* 2018/17, p. 17.

niet afhankelijk is van menselijke arbeid kan een in theorie eindeloze hoeveelheid data worden verzameld. Het risico op stelselmatigheid wordt door deze wijze van zoeken enorm vergroot. Stol en Strikwerda lijken een vergelijkbare mening toegedaan.[100] De regering lijkt zich dit probleem ook gerealiseerd te hebben en heeft om die reden voorgeschreven dat bij algemene maatregel van bestuur nadere regels worden gesteld over de geautomatiseerde wijze van overnemen van gegevens.[101] Daarbij dient het recht op privacy van artikel 8 van het EVRM te worden gewaarborgd.[102]

Diversiteit

De diversiteit van gegevens houdt in dat in een: "*korte tijd veel meer en meer diverse gegevens doorzocht worden dan handmatig in dezelfde tijd en met dezelfde omvang ooit mogelijk zou zijn.*"[103] Dit komt onder andere doordat het gebruik van internet is toegenomen en dat door technologische ontwikkelingen informatiebronnen geautomatiseerd en systematisch geraadpleegd kunnen worden.[104] Dit betekent dat in een mum van tijd grote hoeveelheden data van een persoon kan worden verzameld, waardoor het risico op stelselmatigheid wordt vergroot.

Doel

Bij het doel van de zoekactie wordt nagegaan of het om vastlegging gaat van enkele simpele gerichte feiten of juist breder.[105] Het doel van de zoekactie komt in grote lijnen overeen met de wijze van zoeken. De opsporingsambtenaar kan specifiek op zoek zijn naar online gegevens van een verdachte persoon of hij doet onderzoek naar meerdere al dan niet verdachte personen. Hieruit blijkt dat ondanks de zoekactie doelgericht is, een opsporingsambtenaar gewenst of ongewenst breed kennis kan nemen van een aantal aspecten uit het privéleven van een persoon.

Aard

Wat precies de aard van de persoonsgegevens inhoudt is op dit moment nog niet duidelijk.[106] In de toelichting bij het conceptwetsvoorstel staat dat dit nog moet worden uitgewerkt in de memorie van

[100] Stol & Strikwerda 2017, p. 295.
[101] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 46.
[102] Koops, *JV* 2012/02, p. 30.
[103] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.
[104] Stol & Strikwerda, *TvV* 2018/17, p. 12.
[105] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 164.
[106] Veen, *DD* 2019/30, p. 404.

toelichting.[107] Op grond van het Smartphone arrest kan ik mij voorstellen dat het gaat over de aard van de informatie die een meer dan geringe inbreuk op de privacy van een persoon kan leveren.[108] Uit dit arrest volgt indien volledig inzicht wordt verkregen in de contacten, oproepgeschiedenis, berichten, foto's en video's dat de OvJ of R-C toestemming moet verlenen. Dit komt omdat dan een meer dan geringe inbreuk op de privacy van een persoon wordt gemaakt. De opsporingsambtenaar kan bijvoorbeeld de seksuele geaardheid van iemand achterhalen of dat hij vermoedt dat hij naaktfoto's van iemand gaat vinden, waardoor die aard van de informatie eerder een inbreuk op de privacy oplevert.

Om te kunnen bepalen of het overnemen van persoonsgegevens uit publiek toegankelijke bronnen naar verwachtging stelselmatig zal zijn, hangt van een samenstel van factoren af die hierboven zijn besproken. Bij elk van de factoren is vastgesteld dat deze hogelijk bewerkelijk zijn en dat de toepassing daarvan met onzekerheden is omgeven. Dat betekent dat het op voorhand beoordelen van de (te verwachten) stelselmatigheid op zijn zachtst gezegd een hachelijke onderneming is. Zo zal bij de wijze van zoeken of bij het doel van de zoekactie een risico bestaan dat de opsporingsambtenaar ongewenst breed kennis kan nemen van een aantal aspecten uit het privéleven van een persoon, waardoor vrij snel een inbreuk op de privacy van een persoon kan worden gemaakt. Ook blijkt dat wanneer gebruikt wordt gemaakt van een technisch hulpmiddel van te voren niet goed kan worden vastgesteld hoe groot de inbreuk op de privacy van een persoon zal zijn. De diversiteit aan gegevens speelt hierbij ook een belangrijk rol. Dit komt omdat in een korte tijd diverse gegevens kunnen worden geraadpleegd, waardoor eerder dan voorheen een inbreuk op de privacy kan worden gemaakt. Omdat van te voren niet goed kan worden vastgesteld wat de uitkomst van het samenstel van factoren zal zijn, kan kritiek worden geuit op het toetsingskader van de factoren. Bij een aantal factoren is niet duidelijk wat het beoogde resultaat zal zijn, waardoor een soort van 'grijze ruimte' ontstaat en daarmee een zekere mate van rechtsonzekerheid wordt gecreëerd.

Gezien de grote hoeveelheid factoren is het maar de vraag of een opsporingsambtenaar, een OvJ of een R-C in iedere situatie een juiste afweging kan maken bij de beoordeling van de te verwachten stelselmatigheid.[109] In de memorie van toelichting worden een aantal voorbeelden genoemd wanneer er sprake kan zijn van stelselmatigheid. Als een opsporingsambtenaar de sociale contacten van een persoon op Facebook raadpleegt om vast te kunnen stellen of die persoon een

[107] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 46.
[108] HR 4 april 2017, ECLI:NL:HR:2017:584.
[109] Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *PMSv,* 2018/02, DOI: 10.5553/PMSV/258950952018001018001.

aantal andere personen kent en deze bevindingen vastlegt, is er geen sprake van stelselmatigheid.[110] Mijns inziens is dit niet juist omdat van te voren niet voorspelbaar is hoe groot de verwachte hoeveelheid en wat de aard van de informatie zal zijn. Als gegevens uit een sociaal netwerk worden vastgelegd en worden vergeleken met andere politiegegevens in een netwerkanalyse, is er sprake van stelselmatigheid.[111] Ook bij het herhaaldelijk geautomatiseerd en methodisch zoeken en vastleggen van persoonsgegevens kan van stelselmatigheid sprake zijn.[112]

De regering heeft op advies van de Commissie Koops gekozen voor een algemeen normeringscriterium voor stelselmatigheid. Als gebruik wordt gemaakt van een opsporingsbevoegdheid dan moet worden bepaald of er sprake is van geringe, meer dan geringe en zeer ingrijpende inbreuk op het recht op de persoonlijke levenssfeer. Van stelselmatigheid is sprake als: "*op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan.*"[113] De regering lijkt ervan uit te gaan dat stelselmatigheid te maken heeft met zaken als de hoeveelheid zoekacties, aantal middelen en databanken (kwantitatieve beoordeling), terwijl dit criterium in essentie ziet op de aard van de verzamelde gegevens (kwalitatieve beoordeling).

Aan de hand van algemene en context-specifieke ervaringsregels moet een opsporingsambtenaar een redelijke inschatting maken over de stelselmatigheid. Dat maakt het des te meer wonderlijk en problematisch dat stelselmatigheid op deze wijze wordt vastgesteld. Een opmerkelijk voorbeeld is het volgende. Stel dat de uitoefening van een opsporingsbevoegdheid leidt tot een min of meer volledig beeld van bepaalde aspecten uit het privéleven van een persoon en dat dit op voorhand redelijkerwijs niet was voorzien. Dan is: "*die uitoefening niet met terugwerkende kracht stelselmatig, en is het dus ook niet met terugwerkende kracht onrechtmatig als niet was voldaan aan de desbetreffende vereisten bij stelselmatigheid.*"[114] Hieruit blijkt dus dat onvoorzienbaar aangetroffen gegevens als bijvangst gelden. Deze gegevens mogen als bewijs worden gebruikt.[115] Bij deze werkwijze kunnen vraagtekens gezet worden. Ligthart betoogt dat de ernst van een inbreuk op het recht op privacy van een persoon moet worden beoordeeld aan de hand van de

[110] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[111] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[112] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[113] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.
[114] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.
[115] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.

gegevens die een opsporingsbevoegdheid daadwerkelijk heeft opgeleverd.[116] Een voorbeeld uit het artikel. Op een website wordt illegaal een real-time stream getoond van een webcam op een kamer. De opsporingsambtenaar kijkt tien seconden naar deze stream om vast te stellen of deze kamer is gebruikt voor het maken van kinderporno. De webcam is van een verdachte die een baan heeft met reguliere werktijden. Volgens de Commissie Koops is hier geen sprake van stelselmatigheid. Dit komt omdat niet te verwachten valt dat de verdachte of een huisgenoot overdag gedurende 10 seconden in beeld zal verschijnen.[117] Ligthart stelt daarentegen dat er wel degelijk sprake kan zijn van stelselmatigheid.[118] De verdachte kan bijvoorbeeld net op dat moment toevallig thuiswerken of ziek zijn en naakt de kamer binnenlopen omdat hij op dat moment gedoucht heeft. Ondanks dat deze situatie voor de opsporingsambtenaar niet redelijkerwijs voorzienbaar is, wordt wel een inbreuk op de privacy van een persoon gemaakt. Een probleem waar je tegenaan loopt is de onvoorspelbaarheid van de hoeveelheid en de aard van de gegevens die worden geraadpleegd. Van te voren staat dit niet vast en levert dit problemen op voor de voorzienbaarheid en de proportionaliteit. Wanneer achteraf komt vast te staan dat er wel degelijk sprake is geweest van stelselmatigheid, terwijl dat niet was voorzien, geldt de proportionaliteitstoets niet meer. Het voorzienbaarheidsvereiste geldt ten aanzien van degene tegen wie de opsporingsbevoegdheid wordt ingezet. Het lijkt alsof het voorzienbaarheidsvereiste analoog wordt toegepast op de opsporingsinstantie. Als het voor hen redelijkerwijs niet voorzienbaar is geweest, dan kan blijkbaar het feit dat het voor de verdachte ook niet voorzienbaar is geweest aan de opsporingsinstantie niet worden tegengeworpen.[119]

§ 4.4 Stelselmatigheid in de huidige en nieuwe situatie

Om te kunnen bepalen of er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt zowel in de huidige als in de voorgestelde situatie gebruik gemaakt van het begrip stelselmatigheid. Op grond van artikel 2.8.2.4.1 Sv is van stelselmatigheid sprake als: "*daarbij op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van iemands privéleven.*"[120] De regering beoogt in essentie geen wijziging in de definitie van het begrip stelselmatigheid. Het verschil zit in de wijze waarop die wordt vastgesteld.

---

[116] Ligthart, *RMThemis* 2019, p. 202.
[117] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 48.
[118] Ligthart, *RMThemis* 2019, p. 199.
[119] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.
[120] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 22; Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 38.

Om de stelselmatigheid te kunnen bepalen wordt in de huidige rechtspraak gebruik gemaakt van een samenstel van factoren zoals: de duur, de opslag, de intensiteit, de frequentie en het gebruik van een technisch hulpmiddel.[121] Daarbij is opgemerkt dat de factoren duur en plaats een beperkte relevantie hebben bij het onderzoek naar publiek toegankelijke bronnen. In het wetsvoorstel worden nieuwe factoren voorgesteld. Het samenstel van factoren zoals de wijze van zoeken, de hoeveelheid, de geavanceerdheid, de diversiteit van gegevens, het doel en de aard spelen een belangrijke rol bij de interpretatie van het begrip stelselmatigheid.[122] De voorgestelde factoren zijn beter toepasbaar in de digitale opsporingspraktijk dan de huidige factoren. Een nadeel van de voorgestelde factoren is dat het voor de opsporingsambtenaar vrijwel onmogelijk blijft om van te voren in te schatten of een min of meer volledig beeld van bepaalde aspecten uit het privéleven van een persoon wordt verkregen. Aan de hand van algemene en context-specifieke ervaringsregels moet een opsporingsambtenaar een redelijke inschatting maken van de omstandigheden in het concrete geval, waaronder ook de reeds uit het dossier bekende informatie over een persoon.[123] Hieruit blijkt dat het ondoenlijk is om op voorhand in te schatten of de uitoefening van een bevoegdheid stelselmatig is en is hogelijk privacygevoelige bijvangst een reële mogelijkheid. De opsporingsambtenaar kan bijvoorbeeld informatie verzamelen over de sociale contacten, een bepaalde mening, gevoelens en politieke voorkeur van een persoon.[124]

§ 4.5 Samenvatting

Op grond van artikel 2.8.2.4.1 Sv kan een OvJ bevelen dat een opsporingsambtenaar stelselmatig persoonsgegevens uit publiek toegankelijke bronnen kan overnemen. Van stelselmatigheid is sprake als op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten uit het privéleven van een persoon kan ontstaan. Het begrip stelselmatigheid heeft vrijwel dezelfde betekenis als in de huidige situatie. Om te kunnen bepalen of er sprake is van stelselmatigheid is in de memorie van toelichting een samenstel van factoren ontwikkeld. De bedoeling is dat op basis van deze factoren het omslagpunt wordt bepaald of er sprake is van een meer dan geringe inbreuk op de privacy van een persoon. Een probleem is dat het ondoenlijk is om van te voren een inschatting van de stelselmatigheid te maken, omdat de reikwijdte van de factoren tot onduidelijkheden leidt. Zo kan een eenvoudige zoekvraag op internet tot stelselmatigheid leiden en hoeft bij een onderzoek naar

[121] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27.
[122] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59; *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[123] *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 23.
[124] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.

een grote hoeveelheid gegevens geen sprake te zijn van stelselmatigheid. Het is maar de vraag of de omvang en het type gegevens wel op voorhand valt in te schatten, zeker wanneer geautomatiseerd onderzoek gaat plaatsvinden.

In de memorie van toelichting worden een aantal voorbeelden genoemd van stelselmatigheid. Hieruit blijkt hoe lastig het kan zijn om de stelselmatigheid vast te stellen. Als een opsporingsambtenaar bijvoorbeeld de sociale contacten van iemand raadpleegt om te kijken of deze persoon bepaalde personen kent en hij deze bevindingen vastlegt, is er volgens de regering geen sprake van stelselmatigheid.[125] Wordt daarentegen een sociaal netwerk geanalyseerd en worden deze gegevens vergeleken met politiegegevens om een netwerkanalyse te maken, is er sprake van stelselmatigheid.[126] Per situatie zal een beoordeling van stelselmatigheid moeten plaatsvinden. Geconstateerd kan worden dat de beoordeling van de verwachten stelselmatigheid van het inwinnen van informatie uit publiek toegankelijke bronnen op basis van de voorgestelde factoren nauwelijks mogelijk is en een te hoge onzekerheidsfactor kent.

Tot slot hanteert de regering het eenjaarscriterium bij het wetsvoorstel. Dit betekent dat de opsporingsbevoegdheid uit artikel 2.8.2.4.1 Sv ten aanzien van de huidige situatie vaker kan worden toegepast. Hier ontstaat een discrepantie. Enerzijds lijkt het vaststellen van de stelselmatigheid ondoenlijk, anderzijds vindt er tegelijkertijd een enorme verruiming van de reikwijdte plaats waarbinnen de bevoegdheid kan worden ingezet.

[125] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[126] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.

Hoofdstuk 5 – Het EHRM

§ 5.1 Inleiding

In dit hoofdstuk wordt de inhoud en reikwijdte van artikel 8 van het EVRM geanalyseerd en beschreven. Er wordt stilgestaan bij het toetsingsschema van het EHRM en onderzocht wordt of het voorgestelde wetsartikel 2.8.2.4.1 Sv in overeenstemming is met het toetsingsschema.

§ 5.2 De inhoud en reikwijdte

Artikel 8 van het EVRM is als volgt gedefinieerd:

"1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."[127]

In het EVRM zijn mensen- en burgerrechten opgenomen die gelden voor de lidstaten die zijn aangesloten bij de Raad van Europa.[128] In het eerste lid van artikel 8 van het EVRM wordt het recht op privacy gewaarborgd. Doelstelling van dit artikel is om burgers te beschermen tegen onnodige inmenging door de overheid.[129] Dit is echter geen absoluut recht.[130] In het tweede lid van het artikel wordt een aantal voorwaarden genoemd om van het eerste lid te kunnen afwijken. Zo moet de inbreuk: (1) bij wet voorzien zijn, (2) in het belang zijn van een aantal limitatief opgesomde doelen uit het tweede lid en (3) in een democratische samenleving noodzakelijk zijn.

§ 5.3 Het toetsingsschema van het EHRM

§ 5.3.1 Het toetsingsschema

Het toetsingsschema van het EHRM bestaat uit de volgende elementen:

a. is er sprake van een inbreuk op het recht op privacy;

b. zo ja, is deze in overeenstemming met het recht;

---

[127] Art. 8 EVRM.
[128] Verheugt 2020, p. 560.
[129] EHRM 2 August 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone/Verenigd Koninkrijk*), par. 67; De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 1 (online, bijgewerkt 1 juli 2020).
[130] Keulen & Knigge 2016, p. 93.

c. zo ja, was het doel gerechtvaardigd;

d. zo ja, was de inbreuk noodzakelijk in een democratische samenleving.[131]

§ 5.3.2 Een inbreuk op het recht op privacy

Allereerst wordt onderzocht of er sprake is van een inbreuk op het recht op de privacy. In de jurisprudentie van het EHRM ontbreekt een specifieke omschrijving van het begrip 'recht op privacy'.[132] Per geval moet worden beoordeeld of er sprake is van een inbreuk op dit recht. Met betrekking tot het vaststellen van de privacy inbreuk kan in de meeste gevallen geconcludeerd worden dat er daadwerkelijk sprake is van een inbreuk.[133]

§ 5.3.3 In overeenstemming met het recht (in accordance with the law)

Indien het EHRM van oordeel is dat de overheid een inbreuk heeft gemaakt op het recht op privacy van de klager volgt de tweede voorwaarde. Deze houdt in dat een inbreuk in overeenstemming met het recht moet zijn. Allereerst moet er een grondslag in het nationale recht zijn ('a basis in domestic law'). Zo moet een inbreuk op een grondrecht een wettelijke basis bevatten.[134] Onder het begrip 'law' worden zowel formele als materiële wetten verstaan alsmede jurisprudentie.[135] Daarnaast heeft het EHRM onder andere in de zaak Kruslin tegen Frankrijk geoordeeld dat het nationale recht dient te voldoen aan de kwaliteitseisen die voortvloeien uit de rechtsstaatgedachte ('rule of law').[136] Uit de kwaliteitseisen vloeit voort dat het overheidsoptreden in het nationale recht moet voldoen aan de eisen van toegankelijkheid ('accessibility') en voorzienbaarheid ('foreseeability').[137]

Het toegankelijkheidsvereiste houdt in dat burgers in een lidstaat in staat moeten worden gesteld om wettelijke regelgeving te kunnen raadplegen.[138] Voldoende is dat regelgeving op een eenvoudige wijze geraadpleegd kan worden.

Het voorzienbaarheidsvereiste brengt met zich mee dat het nationale recht rechtszekerheid moet bieden.[139] Daarbij geldt dat het voor een burger voldoende kenbaar moet zijn onder welke

---

[131] Rainey, Wicks & Ovey 2017, p. 343; De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 1 (online, bijgewerkt 1 juli 2020).
[132] Knigge & Kwakman 2001, p. 170.
[133] Harris e.a. 2018, p. 504; Rainey, Wicks & Ovey 2017, p. 401.
[134] Rainey, Wicks & Ovey 2017, p. 343.
[135] De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 4 (online, bijgewerkt 1 juli 2020).
[136] EHRM 24 april 1990, ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin/Frankrijk)*, par. 27; zie ook De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 4. (online, bijgewerkt 1 juli 2020).
[137] Rainey, Wicks & Ovey 2017, p. 343; EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400 (*Weber & Saravia/Duitsland*); EHRM 1 juli 2008, ECLI:CE:ECHR:2008:0701JUD005824300 (*Liberty e.a./ Verenigd Koninkrijk*).
[138] Rainey, Wicks & Ovey 2017, p. 344; EHRM 2 August 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone/Verenigd Koninkrijk*), par. 66.
[139] Rainey, Wicks & Ovey 2017, p. 344.

omstandigheden een inbreuk op de privacy kan worden gemaakt.[140] Uit de rechtspraak van het EHRM vloeien hier twee eisen uit voort. Ten eerste moet in de wet voldoende en duidelijk omschreven zijn onder welke voorwaarden en omstandigheden de overheid een opsporingsbevoegdheid mag toepassen.[141] Ten tweede moet een burger in staat worden gesteld zijn gedrag te reguleren.[142] In beginsel dient een wetsartikel zo nauwkeurig mogelijk te worden geformuleerd. Oftewel, het nationale recht dient met de nodige precisie te zijn geformuleerd.[143] Het EHRM voegt hier aan toe dat niet elke situatie die zich in het recht voor kan doen expliciet in de wet omschreven kan staan.[144] Door continue veranderingen in de samenleving, zoals technologische ontwikkelingen is dit vrijwel onmogelijk omdat de technologie steeds geavanceerder wordt.[145] Derhalve is het onontbeerlijk dat het nationale recht met inachtneming van de grenzen van het EHRM, een discretionaire bevoegdheid overlaat aan de wetgever en aan de rechter.[146]

Tot slot dienen de procedurele waarborgen ('procedural safeguards') in acht te worden genomen door de overheid.[147] Dit betekent dat willekeur voorkomen moet worden en dat een controle mogelijk is op de gebruikte opsporingsbevoegdheid, zodat van deze bevoegdheid geen misbruik kan worden gemaakt. Het EHRM heeft daarbij een duidelijke voorkeur voor een controlemogelijkheid door de rechter.[148]

§ 5.3.4 Een gerechtvaardigd doel (legitimate aim)

De derde voorwaarde uit het toetsingsschema is of het doel gerechtvaardigd is. Het EHRM toetst welke belangen voor de overheid noodzakelijk zijn om een inbreuk op de privacy van burgers te rechtvaardigen.[149] De opsomming uit het tweede lid is limitatief.[150] Zo mag de inbreuk bijvoorbeeld alleen plaatsvinden: "*in het belang van de nationale veiligheid, de openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten."*[151] Omdat de belangen in het tweede lid ruim omschreven zijn, blijkt in de rechtspraktijk dat toetsing aan de derde voorwaarde nauwelijks een

[140] Rainey, Wicks & Ovey 2017, p. 345.
[141] EHRM 21 juni 2011, ECLI:CE:ECHR:2011:0621JUD003019409, (*Shimovolos/Rusland*), par 68.
[142] EHRM 16 februari 2000, ECLI:CE:ECHR:2000:0216JUD002779895 (*Amann/Zwitserland*), par. 56; EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 55.
[143] Rainey, Wicks & Ovey 2017, p. 344.
[144] EHRM 23 september 1998, ECLI:CE:ECHR:1998:0923JUD002475594 (*McLeod/Verenigd Koninkrijk),* par. 41.
[145] EHRM 21 juni 2011, ECLI:CE:ECHR:2011:0621JUD003019409, (*Shimovolos/Rusland*), par 68.
[146] Harteveld e.a. 2004, p. 166.
[147] Rainey, Wicks & Ovey 2017, p. 345.
[148] EHRM 6 juni 2006, ECLI:CE:ECHR:2006:0606JUD006233200 (*Segerstedt-Wiberg e.a./Zweden)*, par. 117; EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 59; Veen, *DD* 2019/30, p. 402.
[149] Rainey, Wicks & Ovey 2017, p. 347.
[150] EHRM 21 februari 1975, ECLI:CE:ECHR:1975:0221JUD000445170 (*Golder/Verenigd Koninkrijk)*, par. 44.
[151] Art. 8 lid 2 EVRM.

belemmering oplevert.[152] Het voorkomen van wanordelijkheden en strafbare feiten zijn de meest ingeroepen doelen en worden door het EHRM het meest geaccepteerd.[153] Dit komt omdat bij de meeste klachten sprake is van een strafrechtelijke maatregel, met als achterliggende doelstelling de preventie van criminaliteit.

§ 5.3.5 De noodzaak in een democratische samenleving (necessary in a democratic society)

De laatste voorwaarde houdt in dat de inbreuk noodzakelijk is een democratische samenleving. Het EHRM oordeelt of de inbreuk door de overheid voorziet in een dringende maatschappelijke behoefte. In onder andere de zaak Silver e.a. tegen het Verenigd Koninkrijk is door het EHRM een aantal aandachtspunten ontwikkeld om te bepalen of er sprake is van een noodzakelijkheid.[154]

Als eerste komt een lidstaat een zekere beoordelingsruimte ('margin of appreciation') toe. Dit betekent dat een lidstaat in het nationale recht een eigen afweging mag maken tussen het recht op privacy en de noodzaak om een doeleinde uit het tweede lid van artikel 8 uit het EVRM te realiseren.[155] Bij deze afweging staat zowel de privacy van een burger als het algemeen belang van de samenleving centraal.

Ten tweede wordt bij de beoordeling van de noodzaak gebruik gemaakt van het proportionaliteits- en subsidiariteitsvereiste. Bij proportionaliteit wordt beoordeeld of het overheidsoptreden in verhouding staat met de gemaakte inbreuk op de privacy van een burger.[156] Bij de subsidiariteit wordt beoordeeld of er minder ingrijpende middelen voor handen waren.[157] Per situatie moet een beoordeling en waarborging plaatsvinden van het recht op de privacy van burgers in een samenleving. Zo werd in de zaak Ribalda e.a. tegen Spanje door het EHRM geoordeeld, dat het gebruik van geheime camera's om diefstal door personeel te ontdekken als disproportioneel bestempeld.[158] Dit kwam onder andere doordat het personeel niet op de hoogte was gesteld van de aanwezigheid van geheime camera's in het gebouw.[159]

Het EHRM geeft een nadere invulling voor de uitwerking van het proportionaliteitsvereiste. Zo dient de gemaakte inbreuk op het recht van de privacy dringend en noodzakelijk te zijn ('pressing social need').[160] Het EHRM toetst vervolgens of de motivering van de overheid om de inbreuk te

---

[152] De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 5 (online, bijgewerkt 1 juli 2020).
[153] Rainey, Wicks & Ovey 2017, p. 353.
[154] EHRM 25 maart 1983, ECLI:CE:ECHR:1983:0325JUD000594772 (*Silver e.a./Verenigd Koninkrijk*); Rainey, Wicks & Ovey 2017, p. 359.
[155] Harris e.a. 2018, p. 14-15.
[156] Harris e.a. 2018, p. 12.
[157] Harris e.a. 2018, p. 17.
[158] EHRM 17 oktober 2019, ECLI:CE:ECHR:2019:1017JUD000187413 (*Ribalda e.a./Spanje*).
[159] EHRM 17 oktober 2019, ECLI:CE:ECHR:2019:1017JUD000187413 (*Ribalda e.a./Spanje*), par. 109-111.
[160] Harris e.a. 2018, p. 12; Rainey, Wicks & Ovey 2017, p. 365.

rechtvaardigen relevant en voldoende bepaalbaar is ('relevant and sufficient').[161] Tevens dient een juiste afweging gemaakt te worden tussen het: "*nagestreefde belang en de wijze waarop er inbreuk is gemaakt op het recht op privacy.*"[162] Dit betekent dat het EHRM nagaat op welke wijze regelgeving is uitgewerkt. In de zaak Zakharov tegen Rusland oordeelde het EHRM dat artikel 8 van het EVRM geschonden was.[163] De regelgeving met betrekking tot het afluisteren van mobiele telefoongegevens had een te ruim toepassingsbereik en er waren geen noodzakelijke procedurele waarborgen in acht genomen. Ook in de zaak Big Brother Watch e.a. tegen Verenigd Koninkrijk oordeelde het EHRM dat er sprake was van een schending van artikel 8 van het EVRM.[164] Er was onder meer sprake van onvoldoende onafhankelijk toezicht op het proces van de selectie van communicatie. Ook was het onduidelijk onder welke omstandigheden overheidsorganen toegang konden aanvragen tot de communicatiegegevens.

Tot slot moeten de adequate waarborgen ('adequate safeguards') in het nationale recht in acht worden genomen.[165] Deze waarborgen dienen ter voorkoming van misbruik van de bevoegdheden, het tegengaan van willekeur en controlemogelijkheden bij de uitvoering van bevoegdheden.

§ 5.4 Het toetsingsschema toegepast op artikel 2.8.2.4.1 Sv

§ 5.4.1 Is er sprake van een inbreuk op het recht op privacy?

De OvJ kan op grond van artikel 2.8.2.4.1 Sv bevelen dat een opsporingsambtenaar stelselmatig persoonsgegevens uit publiek toegankelijke bronnen kan overnemen. Uit de rechtspraak van het EHRM blijkt dat indien persoonlijke gegevens door de overheid worden opgeslagen er zonder meer sprake is van een inbreuk op het recht op privacy.[166] Als een opsporingsambtenaar gebruik maakt van de opsporingsbevoegdheid uit artikel 2.8.2.4.1 Sv is er sprake van een inbreuk, omdat persoonsgegevens worden opgeslagen. Daaruit volgt dat aan de eerste voorwaarde uit het toetsingsschema is voldaan.

[161] Rainey, Wicks & Ovey 2017, p. 365.
[162] De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 6 (online, bijgewerkt 1 juli 2020).
[163] EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (*Zakharov/Rusland*).
[164] EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).
[165] Rainey, Wicks & Ovey 2017, p. 365.
[166] EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*), par. 93; EHRM 6 juni 2006, ECLI:CE:ECHR:2006:0606JUD006233200 (*Segerstedt-Wiberg e.a./Zweden)*, par. 73.

§ 5.4.2 Is de inbreuk in overeenstemming met het recht?

Op grond van artikel 2.8.2.4.1 Sv kan een inbreuk worden gemaakt op het recht op privacy van een persoon. Eerst moet worden beoordeeld of de inbreuk zowel met het nationale recht als met het EVRM in overeenstemming is.[167] Artikel 2.8.2.4.1 Sv is zowel een wet in formele als in materiële zin. Dit betekent dat de wet tot stand is gekomen door de regering en Staten-Generaal en dat dit wetsartikel voor iedereen in de samenleving geldt.[168] Ervan uitgaande dat de opsporingsbevoegdheid in het nieuwe Wetboek van Strafvordering wordt opgenomen, bevat de bevoegdheid een wettelijke grondslag in het nationale recht. Dit betekent dat indien er sprake is van inbreuk op het recht op privacy, deze inbreuk een wettelijke basis bevat.[169]

Uit de literatuur en uit de rechtspraak van het EHRM vloeit voort dat moet worden voldaan aan de eisen van toegankelijkheid en voorzienbaarheid.[170] In het kader van de eis van toegankelijkheid is het van belang dat burgers kennis kunnen nemen van het voorgestelde wetsartikel en dat regelgeving gepubliceerd is. Op dit moment kan het wetsvoorstel en de memorie van toelichting worden geraadpleegd en dat geldt straks zonder meer ook wanneer het artikel in werking treedt. Als het eenmaal in werking treedt dan zal het artikel voldoen aan het toegankelijkheidsvereiste.

De eis van voorzienbaarheid houdt in dat de wet voldoende en duidelijk omschreven moet zijn. Dit betekent dat het voor een burger duidelijk moet zijn onder welke voorwaarden en omstandigheden de overheid bevoegd is om een opsporingsbevoegdheid te mogen toepassen.[171] Daarnaast is een regel voorzienbaar als deze met voldoende precisie is geformuleerd om een burger in staat te stellen zijn gedrag te reguleren.[172] In het wetsvoorstel staat wanneer de opsporingsbevoegdheid kan worden toegepast. Dit kan in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld. In hoofdstuk 4 is vastgesteld dat de factoren wijze van zoeken, hoeveelheid, geavanceerdheid, diversiteit, doel en aard tot onduidelijkheden kunnen leiden bij de vaststelling van stelselmatigheid. Het blijkt bijvoorbeeld dat bij de vaststelling van de aard van de persoonsgegevens niet duidelijk is wat deze factor precies inhoudt. Een eenvoudige zoekopdracht kan bijvoorbeeld tot stelselmatigheid leiden maar bij een onderzoek naar een grote hoeveelheid gegevens hoeft daar geen sprake van te zijn. Dit

---

[167] De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 4 (online, bijgewerkt 1 juli 2020).
[168] Verheugt 2020, p. 9-10.
[169] Rainey, Wicks & Ovey 2017, p. 343.
[170] Rainey, Wicks & Ovey 2017, p. 344; Harteveld e.a. 2004, p. 164; EHRM 26 april 1979,ECLI:CE:ECHR:1979:0426JUD000653874, (*Sunday Times/Verenigd Koninkrijk*); EHRM 17 juli 2003, ECLI:CE:ECHR:2003:0717JUD006373700 (*Perry/Verenigd Koninkrijk)*.
[171] Rainey, Wicks & Ovey 2017, p. 345; EHRM 21 juni 2011, ECLI:CE:ECHR:2011:0621JUD003019409, (*Shimovolos/Rusland*), par 68.
[172] Rainey, Wicks & Ovey 2017, p. 343; EHRM 26 april 1979,ECLI:CE:ECHR:1979:0426JUD000653874, (*Sunday Times/Verenigd Koninkrijk*), par. 49.

terwijl het EHRM wel als eis stelt dat de aard van persoonsgegevens duidelijk omschreven dient te zijn.[173] Tevens blijkt dat het op voorhand inschatten van de omvang en type gegevens van een persoon erg lastig is, zeker bij geautomatiseerd zoeken. Dit komt omdat eerder dan voorheen een min of meer volledig beeld kan worden verkregen over het privéleven van een persoon. Bij toepassing van het samenspel van factoren om de stelselmatigheid te bepalen ontstaat een soort van 'grijze ruimte' waardoor er voor burgers rechtsonzekerheid kan ontstaan. De wet moet voldoende duidelijk zijn zodat het voor een burger helder is onder welke omstandigheden de opsporingsambtenaar gebruik kan maken van de opsporingsbevoegdheid.[174] Het criterium stelselmatig is niet zonder meer duidelijk genoeg om aan de eisen van art. 8 EVRM te voldoen. Echter, in onder andere de zaken Silver[175] en McLeod[176] heeft het EHRM erkend dat het vrijwel onmogelijk is het nationale recht met de nodige precisie te formuleren. De wetgever komt een zekere discretionaire ruimte toe. Hierbij wordt als eis gesteld dat deze bevoegdheid afhankelijk moet worden gemaakt van de ernst van de inbreuk.[177] Doordat de opsporingsbevoegdheid uit artikel 2.8.2.4.1 Sv een meer dan geringe inbreuk op de privacy kan opleveren, is het van belang dat zoveel mogelijk alle gevallen en gronden van die opsporingsbevoegdheid in de wet wordt opgenomen.[178] Belangrijke voorwaarde hierbij is dat burgers hun gedrag kunnen afstemmen op de nieuwe rechtsregels. Het is echter de vraag of het wetsvoorstel hier aan voldoet. Doordat de reikwijdte van de factoren bij het bepalen van de stelselmatigheid niet altijd met voldoende precisie is geformuleerd, is het onduidelijk onder welke omstandigheden de opsporingsbevoegdheid kan worden toegepast. Door deze onduidelijkheden wordt een burger onvoldoende in staat gesteld zijn gedrag te reguleren.

De procedurele waarborgen moeten burgers beschermen tegen misbruik van de bevoegdheden en willekeurige inmenging door de overheid. Daarnaast moeten er controle mogelijkheden zijn op de opsporingsbevoegdheid.[179] Door technologische ontwikkelingen kan eerder dan voorheen in korte tijd ontzettend veel informatie worden verzameld over een persoon. Het EHRM erkent dat door die ontwikkelingen bij het verzamelen van gegevens een risico van willekeur kan ontstaan.[180] Artikel 2.8.2.4.1 Sv stelt als voorwaarde dat alleen in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld, de

[173] EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 57.
[174] EHRM 15 januari 2015, ECLI:CE:ECHR:2015:0115JUD006895511 (*Dragojevic/Kroatië*), par. 81.
[175] EHRM 25 maart 1983, ECLI:CE:ECHR:1983:0325JUD000594772 (*Silver e.a./Verenigd Koninkrijk*), par. 88.
[176] EHRM 23 september 1998, ECLI:CE:ECHR:1998:0923JUD002475594 (*McLeod/Verenigd Koninkrijk)*, par. 41.
[177] EHRM 2 August 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone/Verenigd Koninkrijk*), par. 67.
[178] Harteveld e.a. 2004, p. 172.
[179] Rainey, Wicks & Ovey 2017, p. 345; De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 5 (online, bijgewerkt 1 juli 2020); EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 59.
[180] EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*), par. 114.

OvJ een bevel kan afgeven aan de opsporingsambtenaar. De bevoegde opsporingsambtenaar heeft dan toegang tot persoonsgegevens uit publiek toegankelijke bronnen.[181] Hieruit blijkt dat de OvJ niet willekeurig een opsporingsbevoegdheid kan bevelen. De rechter kan vervolgens als onafhankelijke autoriteit toetsen of de opsporingsbevoegdheid goed is toegepast en in overeenstemming is met het recht.[182] Voorts bedraagt de geldigheidsduur van de opsporingsbevoegdheid maximaal drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd, waarbij de OvJ moet aangeven wat de reden hiervan is.[183] In de zaak Catt tegen het Verenigd Koninkrijk uitte het EHRM zich zeer kritisch uit over de wijze waarop persoonsgegevens in het Verenigd Koninkrijk werden verzameld en opgeslagen.[184] In de wet was niet duidelijk vastgelegd welke gegevens mochten worden geraadpleegd. Volgens het wetsvoorstel mag een opsporingsambtenaar publiek toegankelijke bronnen raadplegen. In de memorie van toelichting wordt de inhoud en reikwijdte daarvan uitgewerkt en toegelicht. Over de aard van het te verzamelen materiaal wordt geen melding gemaakt, terwijl dit wel van belang is.[185] In de memorie van toelichting zou dit nader kunnen worden uitgewerkt. In het wetsvoorstel noch in de memorie van toelichting wordt vermeld hoelang persoonsgegevens bewaard worden.[186] Het EHRM stelt in verband hiermee als eis dat de opslag van gegevens aan een bepaalde termijn is gebonden.[187] De opslag van persoonsgegevens vindt in de huidige rechtspraktijk plaats aan de hand van de Wet bescherming persoonsgegevens en de Wet justitiële en strafvorderlijke gegevens.[188] Op dit moment is het nog niet duidelijk of deze werkwijze in het wetsvoorstel wordt gehanteerd.[189]

Uit het voorgaande blijkt dat bij de voorwaarde van de voorzienbaarheid een aantal problemen aan het licht zijn gekomen. Zo is het niet duidelijk onder welke voorwaarden en omstandigheden de opsporingsbevoegdheid kan worden toegepast, omdat de reikwijdte van de factoren tot onduidelijkheden kunnen leiden. Hierdoor is het voor een burger vrijwel onmogelijk zijn gedrag af te stemmen op de nieuwe rechtsregel. Tevens wordt een aantal procedurele waarborgen in het wetsvoorstel opgenomen. De OvJ kan de opsporingsbevoegdheid bevelen voor een periode van ten hoogste drie maanden en indien nodig kan dit telkens worden verlengd met maximaal drie

[181] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 245.
[182] EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 59.
[183] Veen, *DD* 2019/30, p. 404.
[184] EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*), par. 96-97.
[185] EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië)*, par. 57; Veen, *DD* 2019/30, p. 403.
[186] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 246.
[187] EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*), par. 101.
[188] Commissie modernisering opsporingsonderzoek in het digitale tijdperk. *Regulering van opsporingsbevoegdheden in een digitale omgeving,* s.l. 2018, p. 24.
[189] Veen, *DD* 2019/30, p. 403.

maanden. De rechter kan als onafhankelijke autoriteit controleren of de procedurele waarborgen in acht zijn genomen.

§ 5.4.3 Is het doel gerechtvaardigd?

Op grond van het tweede lid uit artikel 8 van het EVRM moet worden getoetst of de toelaatbaarheid van de inbreuk een gerechtvaardigd doel heeft.[190] Omdat opsporing, vervolging en voorkoming van strafbare feiten de meest ingeroepen doelen zijn, levert dat voor de toetsing van deze voorwaarde vrijwel geen probleem op.[191] In dit geval voldoet het aan de eis van 'legitimate aim'. Dit komt omdat het wetsvoorstel beoogt bij te dragen aan een: "*goed functionerend strafproces dat gekenmerkt wordt door een evenwichtig stelsel van rechtswaarborgen.*"[192] Daarmee zijn zowel het belang van de openbare veiligheid als de voorkoming en vervolging van strafbare feiten gerechtvaardigde doelen voor een noodzakelijke inbreuk op het recht van privacy van een persoon.[193]

§ 5.4.4 Is de inbreuk noodzakelijk?

De laatste voorwaarde houdt in dat de inbreuk op de privacy van een persoon voorziet in een dringende maatschappelijke behoefte. Het beoogde doel van het wetsvoorstel is het waarborgen van de openbare veiligheid en het voorkomen van strafbare feiten. In hoofdstuk 2 is aangegeven dat het huidige Wetboek van Strafvordering nog geen grondslag bevat voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Mede door technologische ontwikkelingen, is vanuit de opsporingspraktijk behoefte aan nieuwe regelgeving.[194] Een lidstaat mag een afweging maken tussen het recht op privacy van een burger en de noodzaak om een van de doeleinden uit het tweede lid van artikel 8 van het EVRM te verwezenlijken in het algemeen belang.[195] Met het wetsvoorstel wordt enerzijds het recht op privacy van een burger beperkt door toepassing van de opsporingsbevoegdheid, anderzijds wordt het algemeen belang van de lidstaat gerealiseerd: het voorkomen van wanordelijkheden en strafbare feiten.[196] Op basis van bovenstaande kan geconcludeerd worden dat aan de 'margin of appreciation' wordt voldaan. In het belang van de openbare veiligheid, de opsporing en vervolging van strafbare feiten is er behoefte aan een

---

[190] De Vocht, in: *T&C Sv* 2019, art. 8 EVRM, aant. 5 (online, bijgewerkt 1 juli 2020).
[191] Rainey, Wicks & Ovey 2017, p. 353.
[192] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 69.
[193] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 76; EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*), par. 108.
[194] *MvT: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 59.
[195] Harris e.a. 2018, p. 14-15.
[196] Rainey, Wicks & Ovey 2017, p. 360.

opsporingsbevoegdheid die kan worden ingezet voor het overnemen van persoonsgegevens uit publiek toegankelijke bronnen.

Met behulp van het proportionaliteits- en subsidiariteitsvereiste wordt getoetst of de inbreuk die het overheidsoptreden heeft veroorzaakt, in balans is met de gemaakte inbreuk op de privacy van een burger.[197] Aan de hand van het proportionaliteitsvereiste moet worden beoordeeld of de wijze van het optreden en het beoogde doel in redelijke balans zijn. Het is echter maar de vraag of de opsporingsbevoegdheid zich verhoudt tot het nagestreefde doel, namelijk het voorkomen van wanordelijkheden en strafbare feiten. De opsporingsbevoegdheid kan bij een grote groep verdachten worden toegepast en door de grote hoeveelheden persoonsgegevens die online beschikbaar zijn, kan de opsporingsambtenaar al gauw een min of meer volledig beeld over iemand zijn privéleven krijgen. Een voorbeeld. Stel iemand vernielt een bankje in het park.[198] Dan kan op grond van het wetsvoorstel de opsporingsbevoegdheid worden toegepast. Dit betekent dat voor relatief lichte strafbare feiten een stelselmatige inbreuk op de privacy kan worden gemaakt. Bovendien kan de opsporingsbevoegdheid ook de privacy van anderen dan de verdachte schenden.
Stel dat een opsporingsambtenaar tijdens een onderzoek online foto's raadpleegt van een feestje waar de plaatselijke dominee nietsvermoedend op de achtergrond zit te zoenen met iemand die niet zijn vrouw is. Dan is zijn privacy evident geschonden en best ingrijpend ook, maar wie houdt dat in de gaten en welke waarborgen zijn er in dat verband? Worden de foto's opgeslagen, wie kan er naar kijken en hoe lang worden ze bewaard? In het wetsvoorstel ontbreken deze waarborgen.

Op grond van het subsidiariteitsvereiste moet het minst bezwarende middel worden gebruikt om de inbreuk op de privacy zoveel mogelijk te beperken.[199] Is er een minder ingrijpend middel voor handen? Wil de opsporingsambtenaar bijvoorbeeld de vriendenkring van de verdachte in kaart brengen dan zou dat ook door middel van observatie of telefoontap kunnen. Deze middelen zijn niet geschikt om het beoogde doel te bereiken, omdat dan een zeer ingrijpende inbreuk op de privacy van een persoon wordt gemaakt.

De 'adequate safeguards' moeten ervoor zorgen dat in het wetsvoorstel voldoende waarborgen worden opgenomen zodat er geen misbruik van de opsporingsbevoegdheid kan worden gemaakt.[200] Een probleem is dat de OvJ niet altijd goed kan inschatten of er een machtiging gegeven moet worden. De waarborg is echter de machtiging zelf. Nu is voor opsporingsbevoegdheden met

[197] Harris e.a. 2018, p. 17; Rainey, Wicks & Ovey 2017, p. 360.
[198] Art. 350 lid 1 Sr.
[199] EHRM 15 januari 2009, ECLI:CE:ECHR:2009:0115JUD003350904 (*Burdov/Rusland*), par. 127; EHRM 18 september 2009, ECLI:CE:ECHR:2009:0918JUD001606490 (*Varnava e.a./Turkije*), par. 164.
[200] Rainey, Wicks & Ovey 2017, p. 365.

een stelselmatig karakter een machtiging van de R-C nodig.[201] Die is meer onafhankelijk van het onderzoek dan de OvJ die immers de leiding heeft over dat onderzoek.[202] Toezicht door een R-C zou in een veel eerder stadium kunnen worden vormgegeven en dat wordt nagelaten. Toezicht achteraf door de zittingsrechter heeft als nadeel dat dan de (ongerechtvaardigde) inbreuk al lang en breed heeft plaatsgevonden. De R-C kan de inbreuk voorkomen. Om de machtiging adequaat te laten functioneren in de opsporingspraktijk moet er een helder toetsingskader zijn. In hoofdstuk 4 is vastgesteld dat dat niet altijd helder is. Een opsporingsambtenaar kan bijvoorbeeld in een bepaalde situatie de stelselmatigheid verkeerd inschatten waardoor hij van mening is dat er sprake is van stelselmatigheid, terwijl die er niet is. Het probleem wordt daarbij nog groter als de beoordeling negatief uitpakt en er ook nog eens geen machtiging wordt afgegeven terwijl dat wel had gemoeten. Een goede beoordeling maken van de stelselmatigheid is nauwelijks mogelijk en als die er is dan stellen de waarborgen weinig voor.

Tot slot is tegenwoordig veel informatie online beschikbaar. Gezien het feit dat een opsporingsambtenaar al vrij snel een min of meer volledig beeld over bepaalde aspecten uit het privéleven van een persoon kan krijgen, verdient het de voorkeur dat een hogere autoriteit zoals de R-C een machtiging kan verlenen.[203] Op deze wijze kan hij een goede controle uitoefenen binnen het opsporingsproces.

Op grond van bovengenoemde uiteenzetting kan geconcludeerd worden dat de inbreuk niet noodzakelijk in een democratische samenleving is. Bij relatief lichte strafbare feiten kan de opsporingsambtenaar gebruik maken van de opsporingsbevoegdheid die al dan niet een inbreuk op de privacy maakt. Daarnaast is de groep personen waarvan de privacy wordt geschonden lastig in te schatten. Niet in alle gevallen is dat proportioneel. In het wetsvoorstel wordt een aantal waarborgen genoemd. De opsporingsbevoegdheid is aan een termijn van drie maanden gebonden en er is vastgelegd welke gegevens geraadpleegd mogen worden om misbruik te voorkomen. Ook vindt er controle mogelijkheid plaats op de uitvoering van de bevoegdheden. Daar staat tegenover dat nog een aantal essentiële waarborgen missen. Het is niet duidelijk hoe de opslag van gegevens plaatsvindt, wie allemaal deze gegevens kan raadplegen en hoe lang deze gegevens bewaard kunnen worden.

[201] Zie ook *Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019, p. 3; *Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* 2017, p. 50.
[202] Art. 148 Sv.
[203] Simmelink, *RMThemis* 2017, p. 325.

§ 5.5 Samenvatting

Een aantal sterkte punten uit het wetsvoorstel is dat de opsporingsbevoegdheid een wettelijke grondslag bevat en het wetsvoorstel voldoende toegankelijk is voor burgers. Een groot nadeel is dat het wetsvoorstel onvoldoende voorzienbaar is. Dit komt omdat de factoren die worden gebruikt om de stelselmatigheid te bepalen tot onduidelijkheden kunnen leiden. Daarnaast is gebleken dat het op voorhand inschatten van de omvang en de hoeveelheid gegevens van een persoon ondoenlijk is, omdat al gauw sprake kan zijn van stelselmatigheid.

Op grond van het proportionaliteitsvereiste kan geconcludeerd worden dat de opsporingsbevoegdheid zich niet goed verhoudt tot het nagestreefde doel: het voorkomen van wanordelijkheden en strafbare feiten. De inbreuk die de opsporingsbevoegdheid veroorzaakt is niet in balans met de gemaakte inbreuk op de privacy van burgers. De bevoegdheid kan nu vaker dan voorheen worden toegepast en ook de privacy van anderen dan de verdachte kan worden geschonden. De 'adequate safeguards' moeten ervoor zorgen dat er geen misbruik van de opsporingsbevoegdheid kan worden gemaakt. Doordat de opsporingsbevoegdheid bij relatief lichte strafbare feiten kan worden toegepast, moet de overheid ervoor zorgen dat er geen risico op willekeur kan ontstaan. Om misbruik van deze bevoegdheid tegen te gaan, moeten de factoren uit de memorie van toelichting voldoende nauwkeurig worden geformuleerd, zodat er een helder toetsingskader voorhanden is. In het wetsvoorstel worden een aantal specifieke waarborgen genoemd ter bescherming van de burger. Het is bijvoorbeeld duidelijk welke gegevens mogen worden geraadpleegd en het bevel wordt gegeven voor een periode van ten hoogste drie maanden. Deze termijn kan telkens met een periode van drie maanden worden verlengd. In theorie zou dit kunnen betekenen dat de opsporingsbevoegdheid langdurig kan worden toegepast. Het is echter wel zo dat de OvJ de verlening moet motiveren. Een nadeel is dat het toetsingskader van de rechterlijke machtiging niet altijd helder is, waardoor onterecht een opsporingsbevoegdheid kan worden afgegeven.

Met het oog op de grote hoeveelheden informatie die opsporingsambtenaren tegenwoordig online kunnen raadplegen, heeft het de voorkeur dat de R-C een machtiging kan afgeven in plaats van de OvJ. De R-C kan meer onafhankelijk worden geacht dan de OvJ omdat die de leiding heeft over het onderzoek. Het onafhankelijke toezicht vindt dan plaats door de R-C, met als slot op de deur een controle achteraf door de rechter.

Hoofdstuk 6 – Conclusie

In dit onderzoek heb ik onderzocht of het criterium van de stelselmatigheid in het voorgestelde artikel 2.8.2.4.1 uit het Wetboek van Strafvordering voldoende helder is en of deze bepaling als geheel in overeenstemming is met artikel 8 van het EVRM. Een vijftal deelvragen zijn gesteld om tot beantwoording van de hoofdvraag te komen. Aan de hand van de bevindingen uit de vorige hoofdstukken wordt in deze conclusie antwoord gegeven op de deelvragen. Tot slot zal antwoord gegeven worden op de hoofdvraag en volgen er enkele aanbevelingen.

De eerste deelvraag van dit onderzoek luidt: *"Welke informatie mag de politie op basis van haar algemene taakstelling online vergaren en van welke bijzondere opsporingsbevoegdheden kan daarnaast gebruik worden gemaakt?"* In hoofdstuk 2 is aan de orde gekomen dat naar huidig recht een opsporingsambtenaar van tevoren een inschatting moet maken of het online vergaren van informatie via de grondslag van artikel 3 Polw moet plaatsvinden of via de artikelen 126g en 126j Sv (bijzondere opsporingsbevoegdheden). Indien de geraadpleegde persoonsgegevens leiden tot een niet meer dan geringe inbreuk op de privacy van een persoon dan kan artikel 3 Polw als grondslag worden gebruikt. Leidt het raadplegen van de persoonsgegevens tot een meer dan geringe inbreuk op de privacy dan kunnen de artikelen 126g en 126j Sv als grondslag worden gebruikt. Aan de hand van een aantal factoren kan worden bepaald of er sprake is van stelselmatigheid. Deze factoren zijn: de duur, de plaats, de intensiteit, de frequentie en het gebruik van een technisch hulpmiddel. Het OM heeft een leidraad ontwikkeld voor opsporingsambtenaren waarin aanwijzingen staan wanneer artikel 3 Polw en de artikelen 126g en 126j Sv als grondslag kunnen worden gebruikt. Op de huidige werkwijze wordt vanuit de opsporingspraktijk en literatuur kritiek geuit, omdat door technologische ontwikkelingen de huidige regelgeving niet goed aansluit bij het online vergaren van informatie.

De tweede deelvraag van het onderzoek is: *"Wat is de achtergrond voor het indienen van het wetsvoorstel?"* Door veranderingen in de samenleving, de toename van het internetgebruik en technologische ontwikkelingen sluiten de wetsbepalingen artikel 3 Polw en de artikelen 126g en 126j Sv niet goed aan bij het huidige digitale tijdperk. Zo kan een opsporingsambtenaar bijvoorbeeld gebruik maken van een geautomatiseerd systeem. Hij kan hiermee binnen enkele muisklikken allerlei persoonlijke informatie over iemand opzoeken, waardoor al gauw een meer dan geringe inbreuk op de privacy van een persoon wordt gemaakt. Door deze digitalisering is vanuit de praktijk behoefte aan een nieuwe opsporingsbevoegdheid om persoonsgegevens uit publiek toegankelijke bronnen over te nemen. Daarnaast zijn de huidige factoren uit memorie van toelichting niet goed toepasbaar om de stelselmatigheid te beoordelen bij het online vergaren van informatie.

De derde deelvraag van dit onderzoek luidt: *"Voor welke problematiek beoogt de voorgestelde bepaling een oplossing te creëren?"* Uit dit onderzoek is gebleken dat het vaststellen van stelselmatigheid op grond van artikel 3 Polw en de bijzondere opsporingsbevoegdheden tot onduidelijkheden kan leiden. Het begrip stelselmatigheid wordt als omslagpunt gebruikt om te beoordelen of er sprake is van een meer dan geringe inbreuk op de privacy van een persoon. Voor een opsporingsambtenaar kan dit lastig zijn omdat van te voren niet duidelijk is welke persoonsgegevens kunnen worden geraadpleegd. Daarnaast ontstaan er problemen bij de bijzondere opsporingsbevoegdheden. Artikel 126j Sv moet worden toegepast wanneer de opsporingsambtenaar gebruikt maakt van misleiding. Bij het online raadplegen van publiek toegankelijke bronnen hoeft hier geen sprake van te zijn, omdat de bron voor een ieder toegankelijk is. Om die reden voldoet de opsporingsbevoegdheid uit art. 126g Sv niet volledig aan deze opsporingshandeling. Bij artikel 126g Sv is er sprake van een 'realtime element'. Indien een opsporingsambtenaar online informatie gaat vergaren, gaat het met name om historische gegevens. Het 'realtime element' is nu niet relevant.

De vierde deelvraag van het onderzoek is: *"Wat is de inhoud en reikwijdte van het begrip stelselmatig?"* Van stelselmatigheid is sprake als op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten uit het privéleven van een persoon kan ontstaan. Om stelselmatigheid te kunnen vaststellen wordt in het wetsvoorstel een aantal factoren vastgesteld. Op basis van deze factoren kan het omslagpunt worden bepaald of er sprake is van een meer dan geringe inbreuk op de privacy van een persoon. Deze factoren zijn: wijze van zoeken, hoeveelheid gegevens, geavanceerdheid, diversiteit, doel en aard. Per situatie zal een beoordeling van de stelselmatigheid moeten plaatsvinden. Uit dit onderzoek blijkt dat de reikwijdte van de factoren bij het bepalen van de stelselmatigheid tot onduidelijkheden kunnen leiden. Bij de wijze van zoeken en het doel van de zoekactie bestaat bijvoorbeeld het risico dat een opsporingsambtenaar onverwacht persoonlijke gegevens kan raadplegen, waardoor hij een meer dan geringe inbreuk op de privacy van een persoon kan maken. Dit komt omdat ontzettend veel persoonlijke gegevens via publiek toegankelijke bronnen raadpleegbaar zijn. Wat precies de aard van de persoonsgegevens inhoudt is op dit moment niet duidelijk, terwijl het EHRM dit wel van belang acht. Voor een opsporingsambtenaar of OvJ is het lastig om van te voren een inschatting te maken van de gevolgen die de inbreuk kan veroorzaken. De reden hiervoor is dat hedendaags grote hoeveelheden informatie direct online beschikbaar is, met als gevolg dat de opsporingsambtenaar onverhoopt privacygevoelige informatie van een persoon in handen kan krijgen. Het is echter de vraag of de omvang en het type gegevens wel op voorhand valt in te schatten, zeker wanneer geautomatiseerd onderzoek gaat plaatsvinden. Ondanks dat de reikwijdte van deze factoren tot onduidelijkheden leiden, zijn de voorgestelde factoren ten aanzien van de huidige factoren overzichtelijker, duidelijker en beter toepasbaar voor het vaststellen van stelselmatigheid.

De laatste deelvraag van dit onderzoek luidt: *"Welke eisen worden ex artikel 8 EVRM gesteld aan een gerechtvaardigde inbreuk op de privacy?"* Op grond van het stappenplan van het EHRM moet artikel 2.8.2.4.1 Sv in overeenstemming met het recht zijn. Geconcludeerd kan worden dat het wetsvoorstel een wettelijke grondslag bevat en aan het toegankelijkheidsvereiste wordt voldaan. Uit het voorzienbaarheidsvereiste vloeit voort dat de wet voldoende en duidelijk omschreven moet zijn en dat een rechtsregel met voldoende precisie geformuleerd moet zijn. In het wetsvoorstel komt duidelijk naar voren wanneer de opsporingsbevoegdheid mag worden toegepast. Echter bij de reikwijdte van de factoren om de stelselmatigheid vast te stellen zijn er onduidelijkheden. Bij het vaststellen van de aard van de persoonsgegevens kan bijvoorbeeld een eenvoudige zoekopdracht al tot stelselmatigheid leiden en bij een onderzoek naar een grote hoeveelheid gegevens hoeft daar geen sprake van te zijn. Daarnaast blijkt dat het op voorhand inschatten van de omvang en type gegevens erg lastig is, omdat dit pas duidelijk wordt wanneer alle publiek toegankelijke bronnen zijn onderzocht. Door deze onduidelijkheden ontstaat een soort van 'grijze ruimte' waardoor een zekere mate van rechtsonzekerheid wordt gecreëerd. Hierdoor is het onduidelijk onder welke omstandigheden de opsporingsbevoegdheid gebruikt kan worden, waardoor de burger onvoldoende in staat wordt gesteld om zijn gedrag af te stemmen op het wetsvoorstel.

De procedurele waarborgen dienen burgers te beschermen tegen willekeurige inmenging van de overheid. Artikel 2.8.2.4.1. Sv bevat een aantal procedurele waarborgen. De OvJ kan niet willekeurig een bevoegdheid afgeven. De OvJ mag slechts een bevel afgeven wanneer er een verdenking van een misdrijf bestaat waarop naar de wettelijke omschrijving een gevangenisstraf van een jaar of meer is gesteld. Daarnaast mag de opsporingsambtenaar drie maanden gebruik maken van de bevoegdheid en kan deze in overleg met de OvJ telkens worden verlengd voor een periode van drie maanden. De rechter kan als onafhankelijke autoriteit toetsen of de opsporingsbevoegdheid goed is toegepast. In het wetsvoorstel ontbreken een aantal waarborgen. Het is niet duidelijk hoe lang gegevens worden opgeslagen en wie kunnen het raadplegen.

Op grond van het tweede lid uit artikel 8 van het EVRM is onderzocht of de voorgestelde opsporingsbevoegdheid een gerechtvaardigd doel heeft. Uit de rechtspraak van het EHRM vloeit voort dat opsporing, vervolging en voorkoming van strafbare feiten de meest ingeroepen doelen zijn. Geconcludeerd kan worden dat de opsporingsbevoegdheid strekt tot het voorkomen van wanordelijkheden en strafbare feiten en dus een gerechtvaardigd doel nastreeft.

Bij de voorwaarde dat de inbreuk 'necessary in a democratic society' moet zijn, blijkt dat het wetsvoorstel niet in overeenstemming is met het proportionaliteitsvereiste. De impact van de opsporingsbevoegdheid op het privéleven van een persoon staat niet altijd in verhouding tot het gepleegde strafbare feit. De bevoegdheid kan namelijk bij een groot aantal strafbare feiten worden toegepast omdat de regering het eenjaarscriterium hanteert in plaats van het voorlopige

hechteniscriterium. Bij relatief lichte strafbare feiten, zoals het vernielen van een bankje in een park, kan de OvJ bevelen dat de opsporingsambtenaar gebruik kan maken van de opsporingsbevoegdheid. Door de grote hoeveelheid persoonsgegevens die online te raadplegen is, levert de opsporingsbevoegdheid al vrij snel een te grote inbreuk op de privacy van een persoon op. Bovendien is de groep personen waarvan de privacy wordt geschonden lastig in te schatten. De R-C staat meer onafhankelijk in het onderzoek dan de OvJ omdat de OvJ de leiding heeft over het onderzoek. Derhalve verdient het de voorkeur dat de R-C als onafhankelijke autoriteit een machtiging afgeeft met als extra waarborg een controle achteraf door de rechter.

Aan het eind van dit onderzoek en met behulp van de antwoorden op de deelvragen kan de hoofdvraag van dit onderzoek worden beantwoord: "*Is het criterium van stelselmatigheid in het voorgestelde artikel 2.8.2.4.1 uit het Wetboek van Strafvordering voldoende helder en is deze bepaling als geheel in overeenstemming met artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden?"* Op basis van dit onderzoek kan worden betoogd dat het criterium van de stelselmatigheid op dit moment niet voldoende helder is. Reden hiervoor is dat de factoren hogelijk bewerkelijk zijn en dat de toepassing daarvan tot onzekerheden leiden. Tot slot kan worden betoogd dat artikel 2.8.2.4.1 Sv als geheel nog niet in overeenstemming is met artikel 8 van het EVRM. Dit komt omdat het toetsingskader van de stelselmatigheid niet voldoende helder is, waardoor niet wordt voldaan aan het voorzienbaarheidsvereiste. Ook is gebleken dat de opsporingsbevoegdheid niet proportioneel is. Doordat deze bevoegdheid eerder dan voorheen kan worden toegepast, levert de opsporingshandeling al vrij snel een inbreuk op de privacy op.

Aanbevelingen

Over een aantal jaar wordt de opsporingsbevoegdheid in het nieuwe Wetboek van Strafvordering opgenomen. Hoewel de regering op de goede weg is, is het mijns inziens nodig dat in een leidraad of in de memorie van toelichting expliciete handvatten worden opgenomen om de stelselmatigheid te kunnen vaststellen. Belangrijk uitgangspunt is dat de factoren eenduidig en overzichtelijk uitgewerkt dienen te worden om op die manier onzekerheden voor de burger te voorkomen. Per factor dient een lijst te worden opgesteld met mogelijke consequenties die de inbreuk kan veroorzaken. Daarnaast wordt in het wetsvoorstel noch in de memorie van toelichting melding gemaakt hoelang persoonlijke gegevens mogen worden bewaard. Gezien de hoeveelheid aan informatie die kan worden vergaard door deze opsporingsbevoegdheid, verdient het de voorkeur om de huidige werkwijze van de opslag van persoonsgegevens te gaan toepassen in het wetsvoorstel. Deze werkwijze is namelijk duidelijk, concreet en overzichtelijk. Tot slot heeft het de voorkeur dat in het wetsvoorstel de R-C de rol van de OvJ gaat overnemen. Gezien de grote hoeveelheid

persoonsgegevens die te vinden zijn op publiek toegankelijke bronnen is het niet proportioneel om bij lichtere strafbare feiten een dergelijk onderzoek te verrichten op bevel van de OvJ. De mate van inbreuk in combinatie met de redelijkheid en voorzienbaarheid vergt een meer onafhankelijke blik, de blik van de R-C.

Literatuurlijst

Blom, in: *T&C Sv* 2019

T. Blom, commentaar op art. 126g Sv, in: C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst & Commentaar Strafvordering*, Deventer: Wolters Kluwer 2019.

Blom, in: *T&C Sv* 2019

T. Blom, commentaar op art. 126j Sv, in: C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst & Commentaar Strafvordering*, Deventer: Wolters Kluwer 2019.

Commissie Koops 2018

Commissie modernisering opsporingsonderzoek in het digitale tijdperk. Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, rijksoverheid.nl/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving.

***Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving* 2019**

Concept-wetsvoorstel en MvT Boek 2 onderdeel opsporing in een digitale omgeving, Den Haag: Ministerie van Justitie en Veiligheid 2019, rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering.

Corstens, Borgers & Kooijmans 2018

G.J.M. Corstens, M.J. Borgers & T. Kooijmans, Het Nederlands Strafprocesrecht, Deventer: Wolters Kluwer 2018.

Eijsbouts e.a. 2020

W.T. Eijsbouts e.a., Europees recht - Algemeen deel, Groningen: Europa Law Publishing 2020.

Harris e.a. 2018

D.J. Harris e.a., *Harris, O'Boyle and Warbrick: Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2018.

Harteveld e.a. 2004

A.E. Harteveld e.a., *Het EVRM en het Nederlandse strafprocesrecht*, Deventer: Kluwer 2004.

Heck, *NRC* 2 januari 2020

W. Heck, 'Universiteit Maastricht betaalde hackers losgeld' *NRC* 2 januari 2020.

Kooijmans, NJ 2018/84

T. Kooijmans, annotatie bij HR 18 december 2018, ECLI:NL:HR:2018:2323, *NJ* 2019/84.

Keulen & Knigge 2016

B.F. Keulen & G. Knigge, Ons strafrecht 2. Strafprocesrecht, Deventer: Wolters Kluwer 2016.

Knigge & Kwakman 2001

G. Knigge & N.J.M. Kwakman, 'Het opsporingsbegrip en de normering van de opsporingstaak' in: Groenhuijsen, M. S., & Knigge, G. (editors*), Het vooronderzoek in strafzaken. Tweede interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Gouda Quint 2001.

Koops, *JV* 2012/02

B.J. Koops, 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *JV* 2012/02, p. 30-46.

Van Krieken, *Strafblad* 2017/14

J.T.F.M. Van Krieken, 'Browsen vanuit rechtersperspectief', *Strafblad*, 2017/14, afl. 4, p. 327-333.

Lassche, in: *Digitalisering en de opsporingspraktijk - juridische aspecten* 2019

H. Lassche, *Digitalisering en de opsporingspraktijk - juridische aspecten*, Apeldoorn: Politieacademie 2019.

Ligthart, *RMThemis* 2019, p. 195-202

S.L.T.J. Ligthart, 'Het criterium van stelselmatigheid in het gemoderniseerde Wetboek van Strafvordering: redelijke voorzienbaarheid als voorwaarde voor meer dan geringe en ingrijpende privacyinbreuken?', *RMThemis* 2019, afl. 5, p. 195-202.

Metselaar, *NRC* 15 januari 2020

D. Metselaar, 'Aantal geregistreerde misdrijven stijgt, vooral meer online misdaad', *NRC* 15 januari 2020.

Moerman, *NJB* 2019/94

E. Moerman, 'Burgers in het digitale opsporingstijdperk', *NJB* 2019/94, afl. 2, p. 112-118.

Oerlemans 2017

J.J. Oerlemans, *Investigating Cybercrime*, Amsterdam: Amsterdam University Press 2017.

Oerlemans 2017

J.J. Oerlemans, *Normering van digitale opsporingsmethoden*, Breda: Nederlandse Defensie Academie 2017.

Oerlemans, *PMSv* 2018/02

J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *PMSv* 2018/02, DOI: 10.5553/PMSV/258950952018001018001.

Oerlemans & Koops, *JV* 2012/05

J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *JV* 2012/05, p. 35-49.

Rainey, Wicks & Ovey 2017

B. Rainey, E. Wicks & C. Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights*, Oxford: Oxford University Press 2017.

Rozendaal & Zuiderveen Borgesius, *Computerrecht* 2017/75

M. Rozendaal & F. Zuiderveen Borgesius, 'Rechter: Usenetprovider moet identificerende gegevens gebruikers verschaffen aan BREIN', *Computerrecht* 2017/75, afl. 2, p. 122.

Simmelink, *RMThemis* 2017, p. 323-333

J.B.H.M. Simmelink, 'Normering van opsporingsbevoegdheden in het gemoderniseerde Wetboek van Strafvordering', *RMThemis* 2017, afl. 6, p. 323-333.

Stol, *TvPol.* 2018/80

W. Stol, 'Politiewerk is … werken in een digitale samenleving', *TvPol.* 2018/80, afl. 5/18, p. 22-25.

Stol & Strikwerda 2017

W. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving,* Den Haag: Boom juridisch 2017.

Stol & Strikwerda, ***TvV* 2018/17**

W. Stol & L. Strikwerda, 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving', *TvV* 2018/17, afl. 1/2, p. 8-22.

***Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering* 2017**

Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering (Het opsporingsonderzoek), Den Haag: Ministerie van Justitie en Veiligheid 2017, rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering.

Veen, *DD* 2019/30

R.S. Veen, 'Digitale opsporing. Het EHRM en het stelselmatige overnemen van persoonsgegevens uit publiek toegankelijke bronnen', *DD* 2019/30, afl. 5, p. 386-404.

Verheugt 2020

J.W.P. Verheugt, Inleiding in het Nederlandse recht, Amsterdam: Uitgeverij De Zuidas 2020.

De Vocht, in: *T&C Sv* 2019

D. de Vocht, commentaar op art. 8 EVRM, in: C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen, *Tekst & Commentaar Strafvordering*, Deventer: Kluwer 2019.

***Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering* 2017**

Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, Den Haag: Ministerie van Justitie en Veiligheid 2017, rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering.

Jurisprudentielijst

Europees Hof voor de Rechten van de Mens

EHRM 21 februari 1975, ECLI:CE:ECHR:1975:0221JUD000445170 (*Golder/Verenigd Koninkrijk)*.

EHRM 26 april 1979,ECLI:CE:ECHR:1979:0426JUD000653874, (*Sunday Times/Verenigd Koninkrijk*).

EHRM 25 maart 1983, ECLI:CE:ECHR:1983:0325JUD000594772 (*Silver e.a./Verenigd Koninkrijk).*

EHRM 2 August 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone/Verenigd Koninkrijk*).

EHRM 24 april 1990, ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin/Frankrijk*).

EHRM 23 september 1998, ECLI:CE:ECHR:1998:0923JUD002475594 (*McLeod/Verenigd Koninkrijk).*

EHRM 16 februari 2000, ECLI:CE:ECHR:2000:0216JUD002779895 (*Amann/Zwitserland*).

EHRM 4 mei 2000, ECLI:CE:ECHR:2000:0504JUD002834195 (*Rotaru/Roemenië*).

EHRM 16 april 2002, ECLI:CE:ECHR:2002:0416JUD003797197 (*Stes Colas Est e.a./Frankrijk*).

EHRM 17 juli 2003, ECLI:CE:ECHR:2003:0717JUD006373700 (*Perry/Verenigd Koninkrijk)*.

EHRM 6 juni 2006, ECLI:CE:ECHR:2006:0606JUD006233200 (*Segerstedt-Wiberg e.a./Zweden*).

EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400 (*Weber & Saravia/Duitsland*).

EHRM 1 juli 2008, ECLI:CE:ECHR:2008:0701JUD005824300 (*Liberty e.a./ Verenigd Koninkrijk*).

EHRM 15 januari 2009, ECLI:CE:ECHR:2009:0115JUD003350904 (*Burdov/Rusland*).

EHRM 18 september 2009, ECLI:CE:ECHR:2009:0918JUD001606490 (*Varnava e.a./Turkije*).

EHRM 21 juni 2011, ECLI:CE:ECHR:2011:0621JUD003019409, (*Shimovolos/Rusland*).

EHRM 15 januari 2015, ECLI:CE:ECHR:2015:0115JUD006895511 (*Dragojevic/Kroatië*).

EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (*Zakharov/Rusland*).

EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*).

EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (*Catt/Verenigd Koninkrijk*).

EHRM 17 oktober 2019, ECLI:CE:ECHR:2019:1017JUD000187413 (*Ribalda e.a./Spanje*).

Hoge Raad

HR 19 december 1995, ECLI:NL:HR:1995:ZD0328.

HR 13 november 2012, ECLI:NL:HR:2012:BW9338.

HR 27 november 2012, ECLI:NL:HR:2012:BY0215.

HR 9 september 2014, ECLI:NL:HR:2014:2650.

HR 12 mei 2015, ECLI:NL:PHR:2015:1018.

HR 4 april 2017, ECLI:NL:HR:2017:584.

HR 6 november 2018, ECLI:NL:HR:2018:2050.

HR 18 juni 2019, ECLI:NL:PHR:2019:648.

Gerechtshof

Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248.

Rechtbank

Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365.